CONTENIDOS DE LA UNIDAD, CRITERIOS DE EVALUACIÓN Y RESULTADOS DE APRENDIZAJE

La siguiente tabla responde al REAL DECRETO 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo. Se incluye también una columna con las unidades didácticas que forman el curso, en las que se desarrollas los diferentes bloques de contenidos.

CONTENIDOS	CRITERIOS DE EVALUACIÓN	RESULTADOS DE APRENDIZAJE	UNIDAD TRABAJO
Bloque 1. Hacking ético, conceptos y herramientas para detección de vulnerabilidades.			
Determinación de las herramientas de monitorización para detectar vulnerabilidades: ▪ Elementos esenciales del hacking ético. ▪ Diferencias entre hacking, hacking ético, tests de penetración y hacktivismo. ▪ Recolección de permisos y autorizaciones previos a un test de intrusión. ▪ Fases del hacking. ▪ Auditorías de caja negra y de caja blanca. ▪ Documentación de vulnerabilidades. ▪ Clasificación de herramientas de seguridad y hacking. ▪ ClearNet, Deep Web, Dark Web, Darknets. Conocimiento, diferencias y herramientas de acceso: Tor, ZeroNet, FreeNet.	a) Se ha definido la terminología esencial del *hacking* ético. b) Se han identificado los conceptos éticos y legales frente al ciberdelito. c) Se ha definido el alcance y condiciones de un test de intrusión. d) Se han identificado los elementos esenciales de seguridad: confidencialidad, autenticidad, integridad y disponibilidad. e) Se han identificado las fases de un ataque seguidas por un atacante. f) Se han analizado y definido los tipos vulnerabilidades. g) Se han analizado y definido los tipos de ataque. h) Se han determinado y caracterizado las diferentes vulnerabilidades existentes. i) Se han determinado las herramientas de monitorización disponibles en el mercado adecuadas en función del tipo de organización.	RA1. Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético.	U.T. 1

Bloque 2. Hacking ético en entornos inalámbricos.			
Ataque y defensa en entorno de pruebas, de las comunicaciones inalámbricas: ▪ Comunicación inalámbrica. ▪ Modo infraestructura, ad-hoc y monitor. ▪ Análisis y recolección de datos en redes inalámbricas. ▪ Técnicas de ataques y exploración de redes inalámbricas. ▪ Ataques a otros sistemas inalámbricos. ▪ Realización de informes de auditoría y presentación de resultados.	a) Se han configurado los distintos modos de funcionamiento de las tarjetas de red inalámbricas. b) Se han descrito las técnicas de encriptación de las redes inalámbricas y sus puntos vulnerables. c) Se han detectado redes inalámbricas y se ha capturado tráfico de red como paso previo a su ataque. d) Se ha accedido a redes inalámbricas vulnerables. e) Se han caracterizado otros sistemas de comunicación inalámbricos y sus vulnerabilidades. f) Se han utilizado técnicas de “Equipo Rojo y Azul”. g) Se han realizado informes sobre las vulnerabilidades detectadas.	RA2. Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades.	U.T. 2
Bloque 3. Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros.			
Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros: ▪ Fase de reconocimiento (footprinting). ▪ Fase de escaneo (fingerprinting). ▪ Monitorizacion de tráfico. ▪ Interceptación de comunicaciones utilizando distintas técnicas. ▪ Manipulación e inyección de tráfico. ▪ Herramientas de búsqueda y explotación de vulnerabilidades. ▪ Ingeniería social. Phising. ▪ Escalada de privilegios.	a) Se ha recopilado información sobre la red y sistemas objetivo mediante técnicas pasivas. b) Se ha creado un inventario de equipos, cuentas de usuario y potenciales vulnerabilidades de la red y sistemas objetivo mediante técnicas activas. c) Se ha interceptado tráfico de red de terceros para buscar información sensible. d) Se ha realizado un ataque de intermediario, leyendo, insertando y modificando, a voluntad, el tráfico intercambiado por dos extremos remotos. e) Se han comprometido sistemas remotos explotando sus vulnerabilidades.	RA3. Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.	U.T. 3

Bloque 4. Consolidación y utilización de sistemas comprometidos.			
Consolidación y utilización de sistemas comprometidos: ▪ Administración de sistemas de manera remota. ▪ Ataques y auditorías de contraseñas. ▪ Pivotaje en la red. ▪ Instalación de puertas traseras con troyanos (RAT, Remote Access Trojan).	a) Se han administrado sistemas remotos a través de herramientas de línea de comandos. b) Se han comprometido contraseñas a través de ataques de diccionario, tablas rainbow y fuerza bruta contra sus versiones encriptadas. c) Se ha accedido a sistemas adicionales a través de sistemas comprometidos. d) Se han instalado puertas traseras para garantizar accesos futuros a los sistemas comprometidos.	RA4. Consolida y utiliza sistemas comprometidos garantizando accesos futuros.	U.T. 4
Bloque 5. Ataque y defensa en entorno de pruebas, de aplicaciones web.			
Ataque y defensa en entorno de pruebas, a aplicaciones web: ▪ Negación de credenciales en aplicaciones web. ▪ Recolección de información. ▪ Automatización de conexiones a servidores web (ejemplo: Selenium). ▪ Análisis de tráfico a través de proxies de intercepción. ▪ Búsqueda de vulnerabilidades habituales en aplicaciones web. ▪ Herramientas para la explotación de vulnerabilidades web.	a) Se han identificado los distintos sistemas de autenticación web, destacando sus debilidades y fortalezas. b) Se ha realizado un inventario de equipos, protocolos, servicios y sistemas operativos que proporcionan el servicio de una aplicación web. c) Se ha analizado el flujo de las interacciones realizadas entre el navegador y la aplicación web durante su uso normal. d) Se han examinado manualmente aplicaciones web en busca de las vulnerabilidades más habituales. e) Se han usado herramientas de búsquedas y explotación de vulnerabilidades web. f) Se ha realizado la búsqueda y explotación de vulnerabilidades web mediante herramientas software.	RA5. Ataca y defiende en entornos de prueba, aplicaciones *web* consiguiendo acceso a datos o funcionalidades no autorizadas.	U.T. 5

C.E. CIBERSEGURIDAD: HACKING ÉTICO

Este módulo profesional contiene la formación necesaria para desempeñar la función de detectar las vulnerabilidades de la organización mediante hacking ético.

La función de hacking incluye aspectos como el ataque programado a las redes y a las aplicaciones web de la organización.

Las actividades profesionales asociadas a esta función se aplican en el ataque de las redes de comunicaciones para acceder a datos o funcionalidades no autorizadas con el propósito de encontrar vulnerabilidades.

La formación del módulo contribuye a alcanzar los objetivos generales ñ), q), r), s), t), u) y v) y las competencias i), k), l), m), n) y ñ) del curso de especialización.

Las líneas de actuación en el proceso de enseñanza aprendizaje que permiten alcanzar los objetivos del módulo versarán sobre:

- Los objetivos y las fases del hacking ético.
- Las herramientas de seguridad y hacking.
- La administración remota de sistemas.
- El ataque ético a redes de comunicaciones, a sistemas y a las aplicaciones web.