TABLA 8: CE y Cb

Resultado de Aprendizaje Criterios de Evaluación					
	RA 1. Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de *hacking* ético.	1. Determinación de las herramientas de monitorización para detectar vulnerabilidades:	Bloque de contenidos	Saber Hacer	Saber Estar
	a) Se ha definido la terminología esencial del hacking ético.	- Elementos esenciales del *hacking* ético. - Diferencias entre *hacking*, *hacking* ético, tests de penetración y hacktivismo. - *ClearNet*, *Deep Web*, *Dark Web*, *Darknets*. Conocimiento, diferencias y herramientas de acceso: *Tor*. *ZeroNet*, *FreeNet*.	Contenidos Básicos	Conoce los diferentes términos relacionados con el hacking ético.	
	b) Se han identificado los conceptos éticos y legales frente al ciberdelito.	- Recolección de permisos y autorizaciones previos a un test de intrusión.		Conoce los coneptos legales y éticos que	Actua de forma ética al detectar vulnerabilidades,

				existen respecto al los delitos informáticos.	
	c) Se ha definido el alcance y condiciones de un test de intrusión.	- Recolección de permisos y autorizaciones previos a un test de intrusión. - Auditorías de caja negra y de caja blanca.		Establece criterios de alcance para realizar un test de intrusión.	
	d) Se han identificado los elementos esenciales de seguridad: confidencialidad, autenticidad, integridad y disponibilidad.	- Recolección de permisos y autorizaciones previos a un test de intrusión.		Identifica los elementos necesarios para realizar un test de intrusión como parte de una auditoría.	
	e) Se han identificado las fases de un ataque seguidas por un atacante	- Fases del *hacking*.		Conoce los procedimientos y las etapas que tiene el proceso de *hacking*.	
	f) Se han analizado y definido los tipos vulnerabilidades.	- Documentación de vulnerabilidades.		Documenta las vulnerabilidades encontradas en un sistema.	

	g) Se han analizado y definido los tipos de ataque.	- Clasificación de herramientas de seguridad y hacking.		Conoce las diferentes técnicas de penetración que existen.	
	h) Se han determinado y caracterizado las diferentes vulnerabilidades existentes.	- Documentación de vulnerabilidades.		Caracteriza y documenta los diferentes tipos de vulnerabilidades.	
	i) Se han determinado las herramientas de monitorización disponibles en el mercado adecuadas en función del tipo de organización	- Clasificación de herramientas de seguridad y hacking.		Clasifica herramientas de monitorización, seguridad y hacking en base a las necesidades.	

Resultado de Aprendizaie	**RA2.** Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades.	4. Ataque y defensa en entorno de pruebas, de las comunicaciones inalámbricas:	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han configurado los distintos modos de funcionamiento de las tarjetas de red inalámbricas.	-Modo infraestructura, ad-hoc y monitor.	Contenidos Básicos	Configura la tarjeta de red del equipo en sus diferentes modos de funcionamiento.	
	b) Se han descrito las técnicas de encriptación de las redes inalámbricas y sus puntos vulnerables.	− Comunicación inalámbrica.		Conoce el funcionamiento de la criptografía en las redes inalámbricas y los estándares que se utilizan en la actualidad de forma comercial.	Valora la importancia de la seguridad de las redes inalámbricas y de usar una tecnología segura en las mismas.
	c) Se han detectado redes inalámbricas y se ha capturado tráfico de red como paso previo a su ataque.	− Análisis y recolección de datos en redes inalámbricas.		Captura e intercepta paquetes de datos en redes inalámbricas.	

	d) Se ha accedido a redes inalámbricas vulnerables.	− Técnicas de ataques y exploración de redes inalámbricas.		Vulnera un punto de acceso inalámbrico	
	e) Se han caracterizado otros sistemas de comunicación inalámbricos y sus vulnerabilidades.	− Ataques a otros sistemas inalámbricos.		Conoce otras tecnologías de red inalámbricas, sus topologías posibles, sus vulnerabiliades y usos más habituales.	
	f) Se han utilizado técnicas de “Equipo Rojo y Azul”.	− Realización de informes de auditoría y presentación de resultados.		Sabe trabajar con la técnica de “Equipo rojo equipo azul” probar la seguridad de un entorno.	
	g) Se han realizado informes sobre las vulnerabilidades detectadas.	− Realización de informes de auditoría y presentación de resultados.		Elabora informes de auditoría sobre las vulnerabiliadades detectadas en un entorno.	

Resultado de Aprendizaie	**RA3.** Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.	3. Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros:	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se ha recopilado información sobre la red y sistemas objetivo mediante técnicas pasivas.	− Fase de reconocimiento (footprinting).	Contenidos Básicos	Recopila información de la red a partir de datos de fuentes abiertas.	Valora el seguimiento de procedimientos a la hora de atacar redes.
	b) Se ha creado un inventario de equipos, cuentas de usuario y potenciales vulnerabilidades de la red y sistemas objetivo mediante técnicas activas.	− Herramientas de búsqueda y explotación de vulnerabilidades. − Ingeniería social. Phising. − Fase de escaneo (fingerprinting).		Realiza un análisis activo de información de la red como equipos, direcciones, usuarios...	
	c) Se ha interceptado tráfico de red de terceros para buscar información sensible.	− Monitorizacion de tráfico. − Interceptación de comunicaciones utilizando distintas técnicas.		Intercepta el tráfico web para descubrir información sobre la red y los sistemas que están en ella.	

	d) Se ha realizado un ataque de intermediario, leyendo, insertando y modificando, a voluntad, el tráfico intercambiado por dos extremos remotos.	− Manipulación e inyección de tráfico.		Realiza un ataque de tipo *man in the middle* modificando el tráfico web entre dos máquinas.	
	e) Se han comprometido sistemas remotos explotando sus vulnerabilidades.	− Escalada de privilegios.		Vulnera un sistema remoto adquiriendo acceso a nivel usuario y privilegiado dentro de una máquina.	

Resultado de Aprendizaje			Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	**RA4.** Consolida y utiliza sistemas comprometidos garantizando accesos futuros.	4. Consolidación y utilización de sistemas comprometidos:	Contenidos Básicos		
	a) Se han administrado sistemas remotos a través de herramientas de línea de comandos.	− Administración de sistemas de manera remota.		Administra sistemas en remoto empleando diferentes tipos de consolas.	
	b) Se han comprometido contraseñas a través de ataques de diccionario, tablas rainbow y fuerza bruta contra sus versiones encriptadas.	− Ataques y auditorías de contraseñas		Utiliza *software* especializado en ataques a contraseñas para vulnerarlas.	Identifica la técnica más adecuada para cada tipo de clave.
	c) Se ha accedido a sistemas adicionales a través de sistemas comprometidos.	− Pivotaje en la red.		Vulnera sistemas no objetivo para acceder a máquinas que contienen la información deseada utilizando técnicas de	

				pivoting o de *pass the hash.*	
	d) Se han instalado puertas traseras para garantizar accesos futuros a los sistemas comprometidos	− Instalación de puertas traseras con troyanos (RAT, Remote Access Trojan).		Compromete sistemas de manera que se puede garantizar su acceso posteriormente.	

Resultado de Aprendizaje	**RA5.** Ataca y defiende en entornos de prueba, aplicaciones *web* consiguiendo acceso a datos o funcionalidades no autorizadas.	5. Ataque y defensa en entorno de pruebas, a aplicaciones *web*:	Bloque de contenidos	Saber Hacer	Saber Estar
Criterios de Evaluación	a) Se han identificado los distintos sistemas de autenticación web, destacando sus debilidades y fortalezas.	− Negación de credenciales en aplicaciones web.	Contenidos Básicos	Conoce y vulnera diferentes tipos de sistemas de autenticación web.	
	b) Se ha realizado un inventario de equipos, protocolos, servicios y sistemas operativos que proporcionan el servicio de una aplicación web.	− Automatización de conexiones a servidores web (ejemplo: Selenium). − Recolección de información		Usa técnicas de enumeración para conocer la arquitectura del *backend* de la aplicación web.	

	c) Se ha analizado el flujo de las interacciones realizadas entre el navegador y la aplicación web durante su uso normal.	− Análisis de tráfico a través de proxies de intercepción.		Implementa *proxies* para capturar el tráfico entre el ordenador y el servidor	Evalua el comportamiento de las aplicaciones web mediante su comportamiento a través de proxies.
	d) Se han examinado manualmente aplicaciones web en busca de las vulnerabilidades más habituales.	− Búsqueda de vulnerabilidades habituales en aplicaciones web.		Detecta vulnerabilidades web habituales analizándo el código y el comportamiento de la misma.	
	e) Se han usado herramientas de búsquedas y explotación de vulnerabilidades web.	− Herramientas para la explotación de vulnerabilidades web.		Automatiza la obtención de vulnerabilidades de una web mediante el uso de *scripts* y herramientas dedicadas.	
	f) Se ha realizado la búsqueda y explotación de vulnerabilidades web mediante herramientas software.	− Herramientas para la explotación de vulnerabilidades web.		Explota vulnerabilidades web.	