



TABLA 9: Evaluación
 Familia Profesional: Informática y Comunicaciones
 Ciclo Formativo: Curso de Especialización en Ciberseguridad en
 Entornos de las Tecnologías de la Información
 Módulo Profesional: Hacking ético

RA1	Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de <i>hacking</i> ético.			20%
%CE	Criterios de evaluación	Instrumento de evaluación		%IE
15	a) Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de <i>hacking</i> ético.	Examen teórico		100
15	b) Se han identificado los conceptos éticos y legales frente al ciberdelito.	Examen teórico		100
10	c) Se ha definido el alcance y condiciones de un test de intrusión.	Trabajo individual		100
10	d) Se han identificado los elementos esenciales de seguridad: confidencialidad, autenticidad, integridad y disponibilidad.	Trabajo individual		50
		FEM		50
10	e) Se han identificado las fases de un ataque seguidas por un atacante	Examen teórico		100
10	f) Se han analizado y definido los tipos vulnerabilidades.	Autoevaluación		100
10	g) Se han analizado y definido los tipos de ataque.	Autoevaluación		100
10	h) Se han determinado y caracterizado las diferentes vulnerabilidades existentes.	Autoevaluación		50
		FEM		50
10	i) Se han determinado las herramientas de monitorización disponibles en el mercado adecuadas en función del tipo de organización	Autoevaluación		100



TABLA 9: Evaluación
Familia Profesional: Informática y Comunicaciones
Ciclo Formativo: Curso de Especialización en Ciberseguridad en
Entornos de las Tecnologías de la Información
Módulo Profesional: Hacking ético

RA2	Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades.		20%
%CE	Criterios de evaluación	Instrumento de evaluación	%IE
5	a) Se han configurado los distintos modos de funcionamiento de las tarjetas de red inalámbricas.	Práctica	100
10	b) Se han descrito las técnicas de encriptación de las redes inalámbricas y sus puntos vulnerables.	Examen teórico	100
15	c) Se han detectado redes inalámbricas y se ha capturado tráfico de red como paso previo a su ataque.	Práctica	50
		FEM	50
20	d) Se ha accedido a redes inalámbricas vulnerables.	Práctica	100
25	e) Se han caracterizado otros sistemas de comunicación inalámbricos y sus vulnerabilidades	Examen teórico	100
15	f) Se han utilizado técnicas de "Equipo Rojo y Azul".	Práctica	100
10	g) Se han realizado informes sobre las vulnerabilidades detectadas.	Práctica	50
		FEM	50

RA3	Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.		20 %
%CE	Criterios de evaluación	Instrumento de evaluación	%IE
20	a) Se ha recopilado información sobre la red y sistemas objetivo mediante técnicas pasivas.	Práctica	50
		FEM	50



TABLA 9: Evaluación
 Familia Profesional: Informática y Comunicaciones
 Ciclo Formativo: Curso de Especialización en Ciberseguridad en
 Entornos de las Tecnologías de la Información
 Módulo Profesional: Hacking ético

RA3	Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.		20 %
%CE	Criterios de evaluación	Instrumento de evaluación	%IE
20	b) Se ha creado un inventario de equipos, cuentas de usuario y potenciales vulnerabilidades de la red y sistemas objetivo mediante técnicas activas.	Práctica	100
20	c) Se ha interceptado tráfico de red de terceros para buscar información sensible.	Práctica	100
20	d) Se ha realizado un ataque de intermediario, leyendo, insertando y modificando, a voluntad, el tráfico intercambiado por dos extremos remotos.	Práctica	100
20	e) Se han comprometido sistemas remotos explotando sus vulnerabilidades.	Práctica	100

RA4	Consolida y utiliza sistemas comprometidos garantizando accesos futuros.		20%
%CE	Criterios de evaluación	Instrumento de evaluación	%IE
25	a) Se han administrado sistemas remotos a través de herramientas de línea de comandos.	Práctica	50
		FEM	50
25	b) Se han comprometido contraseñas a través de ataques de diccionario, tablas rainbow y fuerza bruta contra sus versiones encriptadas.	Práctica	100



TABLA 9: Evaluación
 Familia Profesional: Informática y Comunicaciones
 Ciclo Formativo: Curso de Especialización en Ciberseguridad en
 Entornos de las Tecnologías de la Información
 Módulo Profesional: Hacking ético

RA4	Consolida y utiliza sistemas comprometidos garantizando accesos futuros.		20%
%CE	Criterios de evaluación	Instrumento de evaluación	%IE
25	c) Se ha accedido a sistemas adicionales a través de sistemas comprometidos.	Práctica	100
25	d) Se han instalado puertas traseras para garantizar accesos futuros a los sistemas comprometidos.	Práctica	100

RA5	Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas.		20 %
%CE	Criterios de evaluación	Instrumento de evaluación	%IE
20	a) Se han identificado los distintos sistemas de autenticación web, destacando sus debilidades y fortalezas.	Trabajo individual	50
		FEM	50
20	b) Se ha realizado un inventario de equipos, protocolos, servicios y sistemas operativos que proporcionan el servicio de una aplicación web.	Práctica	50
		FEM	50
15	c) Se ha analizado el flujo de las interacciones realizadas entre el navegador y la aplicación web durante su uso normal.	Práctica	100
15	d) Se han examinado manualmente aplicaciones web en busca de las vulnerabilidades más habituales.	Práctica	100
15	e) Se han usado herramientas de búsquedas y explotación de vulnerabilidades web.	Práctica	100
15	f) Se ha realizado la búsqueda y explotación de vulnerabilidades web mediante herramientas software.	Práctica	100