**Criterios de Evaluación del módulo**

**Hacking Ético**

**Especialización Ciberseguridad**

**Curso: 2021/2022**

**Profesor: Juan Carlos Márquez Llorente**

INDICE:

[1. Criterios de evaluación 3](#_Toc527146299)

[2. Criterios e Instrumentos de Calificación. 6](#_Toc527146300)

# 1. Criterios de evaluación

El currículo del ciclo formativo establece los siguientes resultados de aprendizaje (RA) y sus correspondientes criterios de evaluación (CE):

1. Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético.

Criterios de evaluación:

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.

2. Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades. Criterios de evaluación:

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.

3. Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros. Criterios de evaluación:

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.

4. Consolida y utiliza sistemas comprometidos garantizando accesos futuros. Criterios de evaluación:

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.

5. Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas.

Criterios de evaluación:

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.

# 2. Criterios e Instrumentos de Calificación.

Siguiendo las directrices de la orden 29/07/2010, se vinculan los criterios de evaluación de los distintos resultados de aprendizaje con las diversas unidades de trabajo de tal forma que se evalúan todos los criterios conforme al currículo.

En la siguiente tabla, se especifican por cada resultado de aprendizaje, cuáles son sus criterios de evaluación indicando que unidades de trabajo los contemplan y que instrumentos de evaluación emplearemos para medir el grado de consecución. Por último, se indica el peso de cada criterio sobre el resultado de aprendizaje.

|  |  |  |
| --- | --- | --- |
| **RESULTADO DE APRENDIZAJE** | **U.T.** | **% ASIGNADO A CADA R.A.****(SOBRE UN 100%)** |
| R.A. 1.Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético. | 1 | 20% |
| R.A. 2.Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades | 2 | 20% |
| R.A. 3.Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros. | 3 | 20% |
| R.A. 4.Consolida y utiliza sistemas comprometidos garantizando accesos futuros. | 4 | 10% |
| R.A. 5.Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas | 5 | 30% |
|  | TOTAL | 100% |

**Criterios de calificación**

Para realizar la evaluación de los criterios de evaluación mencionados en la tabla anterior, se disponen de una serie de instrumentos de evaluación para evaluar cada criterio. Así se utilizarán habitualmente prácticas que evaluarán un conjunto de criterios y puntualmente pruebas escritas o exámenes. **Las pruebas escritas se realizarán al final de cada trimestre en una fecha determinada y los alumnos sabrán en todo momento qué criterios de evaluación se van a incluir en la prueba escrita.**

|  |  |
| --- | --- |
| Instrumentos de evaluación de cada unidad de trabajo | Porcentaje |
| Pruebas realizadas en el trimestre en las cuales el alumno demuestra la correcta asimilación de las materias impartidas. | 50 % |
| Participación en el día a día, en los foros | 10% |
| Actividades de enseñanza-aprendizaje, consistentes en prácticas, ejercicios o trabajos propuestos por el profesor a los alumnos. | 20 % |

Es conveniente indicar que los criterios de evaluación se van a evaluar a través de una práctica y/o de pruebas escritas. En el caso de que un criterio sea evaluable con dos instrumentos de evaluación se hará una media ponderada en base al porcentaje de los distintos instrumentos de evaluación.

Durante el desarrollo de la unidad de trabajo correspondiente se le indicara al alumno los criterios de evaluación asociados a esa unidad de trabajo. Además, se indicará el instrumento o instrumentos (examen o práctica) que se va a emplear para evaluar dicho criterio de evaluación.

Para realizar la calificación del alumno, se tendrá en cuenta el peso de cada unidad de trabajo mostrado anteriormente, realizando una media ponderada en base al peso de cada unidad de trabajo.

**IMPORTANTE:**

**PARA APROBAR CADA TRIMESTRE HAY QUE OBTENER UNA CALIFICACIÓN NUMÉRICA DE 5 O SUPERIOR, SIENDO ADEMÁS OBLIGATORIO LA ENTREGA DE TODOS LOS TRABAJOS ENCOMENDADOS POR EL PROFESOR.**

**Para aquellos alumnos que no hayan podido entregar los trabajos en el periodo indicado se abrirá un plazo (indicado con antelación suficiente) dónde podrán entregar las prácticas pendientes. La calificación de estos trabajos será de APTO o NO APTO.**

**Es requisito indispensable para la superación del módulo que el alumno supere cada de los criterios de evaluación asociados a cada uno de los resultados de aprendizaje del módulo de acuerdo con los criterios de calificación establecidos.**

PARA APROBAR EL MODULO COMPLETO HAY QUE OBTENER UNA CALIFICACIÓN NUMERICA DE 5 PUNTOS O SUPERIOR.