**Programación didáctica del módulo:**

**Hacking Ético**

**Curso de especialización: Ciberseguridad en Entornos de las Tecnologías**

**Curso: 2023/2024**

**Profesor:**

**Ignacio Gómez de Parada López**

**Índice**

1. Criterios de evaluación 3

2. Criterios de calificación 3

3. Recuperación 6

#

## Criterios de evaluación

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

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.

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.

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.

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.

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.

## Criterios de calificación

Dado el carácter práctico de la Formación Profesional, se establece una calificación mixta entre los contenidos evaluados en proyectos y en los exámenes, si bien todos los exámenes evalúan en un porcentaje muy elevado la realización de actividades prácticas en el tiempo fijado.

En cada una de las evaluaciones se calificarán los siguientes conceptos:

* Una actividad de enseñanza-aprendizaje (proyectos o trabajos realizados por el alumno): 40% de la nota.
* Un examen escrito con contenido teórico y práctico por cada unidad de trabajo: 60% de la nota.

Sin embargo, para superar cada evaluación es necesario:

* Haber obtenido al menos un 4,5 en **cada uno** de los exámenes escritos con contenido práctico y en cada una de las actividades de enseñanza-aprendizaje.
* Haber obtenido al menos un 4,5 sobre 10 en la nota de cada evaluación.

**No se considera la evaluación superada si no se cumplen los dos criterios anteriores.**

|  |
| --- |
| **El alumno deberá superar cada una de las evaluaciones del curso. La nota final del módulo corresponde a la media aritmética de la nota obtenida en las evaluaciones, en el caso de que todas ellas estén aprobadas.** **Si el alumno no supera una o varias evaluaciones, la nota final será de suspenso.** |

Alumnos con pérdida de la Evaluación Continua Y Alumnos con Evaluación continua que no superen el módulo.

Dado el carácter práctico de la Formación Profesional, se establece una calificación

Realizarán una prueba final que supondrá el 100% de la calificación, estado está comprendida entre 1-10. El alumno deberá obtener una calificación final igual o superior a 5 sobre 10 para superar el módulo.

## Recuperación

Si un alumno no supera una o varias evaluaciones, deberá recuperar las evaluaciones no superadas en el examen final de recuperación que se realizará en la primera convocatoria ordinaria.

En el examen final de la primera convocatoria ordinaria, el alumno deberá recuperar **únicamente** aquellas evaluaciones no superadas. En el caso de no recuperar las evaluaciones suspensas, la calificación final será de suspenso.

Para poder aprobar los exámenes suspensos, el estudiante se podrá presentar a un segundo examen que abarque el mismo temario en el mismo trimestre o al principio del siguiente. Si volviesen a suspender el examen, se podrá presentar al examen de la primera y en caso necesario, la segunda ordinaria para poder presentarse a otro examen sólo con las materias suspensas.

Acceso a la segunda convocatoria ordinaria

Los alumnos que, después de la primera convocatoria tengan módulos no superados, accederán a la segunda convocatoria de cada curso académico. No obstante, si el alumno no se presenta a las pruebas de evaluación preparadas por los profesores para la segunda convocatoria, se entenderá que el alumno renuncia a la misma, sin necesidad de haberlo solicitado previamente.

El acceso a la segunda convocatoria ordinaria se realizará independientemente del tipo de matrícula del alumno (ordinaria o modular).

Antes de la realización de la segunda convocatoria ordinaria si el profesor lo considera oportuno se programarán ejercicios de recuperación que se deberán de entregar en la fecha establecida por cada profesor.

El examen de la segunda convocatoria ordinaria incluirá solo aquellos contenidos que no se hayan conseguido superar en la primera.

 La segunda convocatoria ordinaria se realizará en el mes de Junio.

**Planificación de las actividades de recuperación de los módulos no superados**

 Dado que se utiliza la plataforma Moodle a lo largo del módulo/asignatura, los alumnos tienen a su disposición el conjunto de ejercicios que les pueden servir de refuerzo para superar el examen de la segunda convocatoria ordinaria

 Se realizará una prueba final por cada una de las convocatorias ordinarias, esta prueba supondrá el 60% de la calificación y las tareas, aunque se entreguen en el plazo extraordinario supondrán el otro 40% de la calificación. El alumno deberá obtener una calificación final igual o superior a 5 sobre 10 para superar el módulo.