TABLA 11: Unidades de Aprendizaje

(Una por cada Unidad)

Unidad de Aprendizaje Nº 1 Introducción al hacking. Definiciones y consideraciones.		
Temporalización: Semana 1ª- 3ª	**Duración**: 12h	**Ponderación**: 10%

Objetivos Generales	Competencias
ñ) Combinar técnicas de hacking ético interno y externo para detectar vulnerabilidades que permitan eliminar y mitigar los riesgos asociados. **q) Desarrollar manuales de información utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.** **r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación para mantener el espíritu de actualización y**	**i) Detectar vulnerabilidades en sistemas, redes y aplicaciones, evaluando los riesgos asociados.** **k) Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente respondiendo a los requisitos establecidos.** **l) Adaptarse a las nuevas situaciones laborales manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida.**

adaptarse a nuevas situaciones laborales y personales. s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal. t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo para garantizar entornos seguros. u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas». v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje para valorar la cultura de la evaluación y de la calidad y ser	m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo. n) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización. ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.

capaces de supervisar y mejorar procedimientos de calidad.	

Resultados de Aprendizaje	
1. Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético.	
Aspectos del Saber Hacer	**Aspectos del Saber**
Conoce los diferentes términos relacionados con el hacking ético. Conoce los coneptos legales y éticos que existen respecto al los delitos informáticos. Establece criterios de alcance para realizar un test de intrusión. Identifica los elementos necesarios para realizar un test de intrusión como parte de una auditoría.	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. Recolección de permisos y autorizaciones previos a un test de intrusión. Recolección de permisos y autorizaciones previos a un test de intrusión.
Aspectos del Saber Estar	
Actua de forma ética al detectar vulnerabilidades.	Auditorías de caja negra y de caja blanca. Recolección de permisos y autorizaciones previos a un test de intrusión.

Tareas y Actividades		
• Se va a hacer una introducción a los conceptos relacionados con el *hacking*. • De igual modo se explicarán los conceptos éticos básicos relacionados con la disciplina. • Se definirá lo que es un test de intrusión y todo aquello vinculado a realizar uno desde el punto de vista legal.		
Criterios de Evaluación	**%**	**IE**
1.a) Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético.	15	Examen teórico
1.b) Se han identificado los conceptos éticos y legales frente al ciberdelito.	15	Examen teórico
1.c) Se ha definido el alcance y condiciones de un test de intrusión.	10	Trabajo individual
1.d) Se han identificado los elementos esenciales de seguridad: confidencialidad, autenticidad, integridad y disponibilidad.	10	Trabajo individual (50%) FEM (50%)
Recursos		
Aula-taller con ordenadores para cada uno de los alumnos de la clase. Los equipos deberán contar con herramientas de ofimática básicas, software de virtualización y suficiente memoria y disco duro como para poder virtualizar varias máquinas de forma rápida. Una pantalla o proyector.		
Observaciones		

Unidad de Aprendizaje Nº 2 **Inicio de hacking, máquinas, redes y aprovechamiento de vulnerabilidades conocidas.**		
Temporalización: Semana 4ª- 10ª	**Duración**: 30 h	**Ponderación**: 25%

Objetivos Generales	Competencias
ñ) Combinar técnicas de hacking ético interno y externo para detectar vulnerabilidades que permitan eliminar y mitigar los riesgos asociados. **q) Desarrollar manuales de información utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.** **r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales.**	**i) Detectar vulnerabilidades en sistemas, redes y aplicaciones, evaluando los riesgos asociados.** **k) Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente respondiendo a los requisitos establecidos.** **l) Adaptarse a las nuevas situaciones laborales manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida.** **m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en**

s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal. t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo para garantizar entornos seguros. u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas». v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.	el ámbito de su competencia con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo. n) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización. ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.
Resultados de Aprendizaje	

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

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

4. Consolida y utiliza sistemas comprometidos garantizando accesos futuros.

Aspectos del Saber Hacer	Aspectos del Saber
Conoce los procedimientos y las etapas que tiene el proceso de hacking. Documenta las vulnerabilidades encontradas en un sistema. Conoce las diferentes técnicas de penetración que existen. Caracteriza y documenta los diferentes tipos de vulnerabilidades. Clasifica herramientas de monitorización, seguridad y hacking en base a las necesidades. Recopila información de la red a partir de datos de fuentes abiertas. Realiza un análisis activo de información de la red como equipos, direcciones, usuarios...	Fases del hacking. Documentación de vulnerabilidades. Clasificación de herramientas de seguridad y hacking. Documentación de vulnerabilidades. Clasificación de herramientas de seguridad y hacking. Fase de reconocimiento (*footprinting*). Herramientas de búsqueda y explotación de vulnerabilidades. Ingeniería social. *Phising*. Fase de escaneo (*fingerprinting*). 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. Realiza un ataque de tipo *man in the middle* modificando el tráfico web entre dos máquinas. Vulnera un sistema remoto adquiriendo acceso a nivel usuario y privilegiado dentro de una máquina. Administra sistemas en remoto empleando diferentes tipos de consolas. Utiliza software especializado en ataques a contraseñas para vulnerarlas. Vulnera sistemas no objetivo para acceder a máquinas que contienen la información deseada utilizando técnicas de pivoting o de pass the hash. Compromete sistemas de manera que se puede garantizar su acceso posteriormente.	Manipulación e inyección de tráfico. Escalada de privilegios. 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).
Aspectos del Saber Estar	

Identifica la técnica más adecuada para cada tipo de clave. Valora el seguimiento de procedimientos a la hora de atacar redes.	

Tareas y Actividades
• Se explicarán en el aula las fases del hacking. • Se realizarán prácticas de enumeración, bien sea con máquinas virtualizadas o servidores reales. • Se buscarán y aprovecharán las vulnerabilidades descubiertas en la enumeración. • Se conseguirá acceso a máquinas remotas. • Se utilizarán técnicas de ingeniería social y ataques *man in the middle* en entornos de prueba. • Se realizarán ataques de diccionario y fuerza bruta a contraseñas. • Se realizarán prácticas de monitorización del tráfico e inyección de código. • Se instalarán puertas traseras en las máquinas vulneradas. • Se realizará una práctica de pivoting entre varias máquinas.

Criterios de Evaluación	%	IE
1.e) Se han identificado las fases de un ataque seguidas por un atacante.	10	Autoevaluación
1.f) Se han analizado y definido los tipos vulnerabilidades.	10	Autoevaluación
1.g) Se han analizado y definido los tipos de ataque	10	Autoevaluación
1.h) Se han determinado y caracterizado las diferentes vulnerabilidades existentes.	10	Autoevaluación (50%)

		FEM (50%)
1.i) Se han determinado las herramientas de monitorización disponibles en el mercado adecuadas en función del tipo de organización.	10	Autoevaluación
3.a) Se ha recopilado información sobre la red y sistemas objetivo mediante técnicas pasivas.	20	Práctica
3.b) Se ha creado un inventario de equipos, cuentas de usuario y potenciales vulnerabilidades de la red y sistemas objetivo mediante técnicas activas.	20	Práctica
3.c) Se ha interceptado tráfico de red de terceros para buscar información sensible.	20	Práctica
3.d) Se ha realizado un ataque de intermediario, leyendo, insertando y modificando, a voluntad, el tráfico intercambiado por dos extremos remotos.	20	Práctica
3.e) Se han comprometido sistemas remotos explotando sus vulnerabilidades.	20	Práctica
4.a) Se han administrado sistemas remotos a través de herramientas de línea de comandos.	25	Práctica (50%) FEM (50%)
4.b) Se han comprometido contraseñas a través de ataques de diccionario, tablas rainbow y fuerza bruta contra sus versiones encriptadas.	25	Práctica
4.c) Se ha accedido a sistemas adicionales a través de sistemas comprometidos.	25	Práctica
4.d) Se han instalado puertas traseras para garantizar accesos futuros a los sistemas comprometidos.	25	Práctica
Recursos		
Aula-taller con ordenadores para cada uno de los alumnos de la clase.		

Los equipos deberán contar con herramientas de ofimática básicas, software de virtualización y suficiente memoria y disco duro como para poder virtualizar varias máquinas de forma rápida. Una pantalla o proyector.
Observaciones

Unidad de Aprendizaje Nº 3 **Hacking aplicaciones web**		
Temporalización: Semana 11ª-16ª	**Duración**: 24h	**Ponderación**: 20%

Objetivos Generales	Competencias
ñ) Combinar técnicas de hacking ético interno y externo para detectar vulnerabilidades que permitan eliminar y mitigar los riesgos asociados. **q) Desarrollar manuales de información utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.**	**i) Detectar vulnerabilidades en sistemas, redes y aplicaciones, evaluando los riesgos asociados.** **k) Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente respondiendo a los requisitos establecidos.** **l) Adaptarse a las nuevas situaciones laborales manteniendo actualizados los**

r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales. s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal. t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo para garantizar entornos seguros. u) Identificar y proponer las acciones profesionales necesarias para dar respuesta	conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida. m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo. n) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización. ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los

a la accesibilidad universal y al «diseño para todas las personas». **v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.**	**procesos de producción o prestación de servicios.**

Resultados de Aprendizaje	
1. Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético. **5. Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas.**	
Aspectos del Saber Hacer	**Aspectos del Saber**
Conoce los procedimientos y las etapas que tiene el proceso de hacking. Documenta las vulnerabilidades encontradas en un sistema. Conoce las diferentes técnicas de penetración que existen. Caracteriza y documenta los diferentes tipos de vulnerabilidades.	Fases del hacking. Documentación de vulnerabilidades. Clasificación de herramientas de seguridad y hacking. Documentación de vulnerabilidades. Clasificación de herramientas de seguridad y hacking. Negación de credenciales en aplicaciones web.

Clasifica herramientas de monitorización, seguridad y hacking en base a las necesidades. Conoce y vulnera diferentes tipos de sistemas de autenticación web. Usa técnicas de enumeración para conocer la arquitectura del backend de la aplicación web. Implementa proxies para capturar el tráfico entre el ordenador y el servidor Detecta vulnerabilidades web habituales analizándo el código y el comportamiento de la misma. Automatiza la obtención de vulnerabilidades de una web mediante el uso de scripts y herramientas dedicadas. Explota vulnerabilidades web.	Automatización de conexiones a servidores web (ejemplo: Selenium). Recolección de información Análisis de tráfico a través de proxies de intercepción. Búsqueda de vulnerabilidades habituales en aplicaciones web. Herramientas para la explotación de vulnerabilidades web. Herramientas para la explotación de vulnerabilidades web.
Aspectos del Saber Estar	
Evalua el comportamiento de las aplicaciones web mediante su comportamiento a través de proxies.	

Tareas y Actividades		
• Se estudiarán los tipos de ataques más habituales a servicios web y se realizarán prácticas en las que se pongan a prueba y se desarrollen los conocimientos. DDoS, XSS, SSTI... • Se flitrará el tráfico entre el navegador y el servidor para su análisis. • Se atacará a los sistemas de autentificación web. • Se usarán herramientas que automaticen la búsqueda de vulnerabilidades web.		
Criterios de Evaluación	**%**	**IE**
1.e) Se han identificado las fases de un ataque seguidas por un atacante.	10	Autoevaluación
1.f) Se han analizado y definido los tipos vulnerabilidades.	10	Autoevaluación
1.g) Se han analizado y definido los tipos de ataque	10	Autoevaluación
1.h) Se han determinado y caracterizado las diferentes vulnerabilidades existentes.	10	Autoevaluación (50%) FEM (50%)
1.i) Se han determinado las herramientas de monitorización disponibles en el mercado adecuadas en función del tipo de organización.	10	Autoevaluación
5.a) Se han identificado los distintos sistemas de autenticación web, destacando sus debilidades y fortalezas	20	Trabajo individual (50%) FEM (50%)
5.b) Se ha realizado un inventario de equipos, protocolos, servicios y sistemas operativos que proporcionan el servicio de una aplicación web.	20	Práctica (50%) FEM (50%)
5.c) Se ha analizado el flujo de las interacciones realizadas entre el navegador y la aplicación web durante su uso normal.	15	Práctica

5.d) Se han examinado manualmente aplicaciones web en busca de las vulnerabilidades más habituales.	15	Práctica
5.e) Se han usado herramientas de búsquedas y explotación de vulnerabilidades web.	15	Práctica
5.f) Se ha realizado la búsqueda y explotación de vulnerabilidades web mediante herramientas software.	15	Práctica

Recursos

Aula-taller con ordenadores para cada uno de los alumnos de la clase.

Los equipos deberán contar con herramientas de ofimática básicas, software de virtualización y suficiente memoria y disco duro como para poder virtualizar varias máquinas de forma rápida.

Una pantalla o proyector.

Observaciones

Unidad de Aprendizaje Nº 4 **Hacking redes inalámbricas**		
Temporalización: Semana 17ª-20ª	**Duración**: 18h	**Ponderación**: 15%

Objetivos Generales	Competencias

ñ) Combinar técnicas de hacking ético interno y externo para detectar vulnerabilidades que permitan eliminar y mitigar los riesgos asociados. q) Desarrollar manuales de información utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa. r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales. s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal. t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental	i) Detectar vulnerabilidades en sistemas, redes y aplicaciones, evaluando los riesgos asociados. k) Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente respondiendo a los requisitos establecidos. l) Adaptarse a las nuevas situaciones laborales manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida. m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo. n) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo supervisando y aplicando los procedimientos de

proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo para garantizar entornos seguros. **u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».** **v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.**	**prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización.** **ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.**

Resultados de Aprendizaje	
1. Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético. **2. Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades.**	
Aspectos del Saber Hacer	**Aspectos del Saber**
Conoce los procedimientos y las etapas que tiene el proceso de hacking.	Fases del hacking. Documentación de vulnerabilidades.

Documenta las vulnerabilidades encontradas en un sistema. Conoce las diferentes técnicas de penetración que existen. Caracteriza y documenta los diferentes tipos de vulnerabilidades. Clasifica herramientas de monitorización, seguridad y hacking en base a las necesidades. Configura la tarjeta de red del equipo en sus diferentes modos de funcionamiento. Conoce el funcionamiento de la criptografía en las redes inalámbricas y los estándares que se utilizan en la actualidad de forma comercial. Captura e intercepta paquetes de datos en redes inalámbricas. Vulnera un punto de acceso inalámbrico Conoce otras tecnologías de red inalámbricas, sus topologías	Clasificación de herramientas de seguridad y hacking. Documentación de vulnerabilidades. Clasificación de herramientas de seguridad y hacking. Modo infraestructura, ad-hoc y monitor. Comunicación inalámbrica. 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. Realización de informes de auditoría y presentación de resultados.

posibles, sus vulnerabiliades y usos más habituales. Sabe trabajar con la técnica de "Equipo rojo equipo azul" probar la seguridad de un entorno. Elabora informes de auditoría sobre las vulnerabiliadades detectadas en un entorno.	
Aspectos del Saber Estar	
Valora la importancia de la seguridad de las redes inalámbricas y de usar una tecnología segura en las mismas.	

Tareas y Actividades

- Se describirán los diferentes niveles de seguridad inalámbrica y los métodos de vulnerarlos.
- Se realizará una práctica de captura de tráfico inalámbrico y concexión a un punto de acceso.
- Se describirán otras tecnologías inalámbricas y se accederá a las mismas.
- Se realizarán prácticas de vulneración de tarjetas con la tecnología MiFare Classic.

Criterios de Evaluación	%	IE
1.e) Se han identificado las fases de un ataque seguidas por un atacante.	10	Autoevaluación
1.f) Se han analizado y definido los tipos vulnerabilidades.	10	Autoevaluación
1.g) Se han analizado y definido los tipos de ataque	10	Autoevaluación

1.h) Se han determinado y caracterizado las diferentes vulnerabilidades existentes.	10	Autoevaluación (50%) FEM (50%)
1.i) Se han determinado las herramientas de monitorización disponibles en el mercado adecuadas en función del tipo de organización.	10	Autoevaluación
2.a) Se han configurado los distintos modos de funcionamiento de las tarjetas de red inalámbricas.	5	Práctica
2.b) Se han descrito las técnicas de encriptación de las redes inalámbricas y sus puntos vulnerables.	10	Examen teórico
2.c) Se han detectado redes inalámbricas y se ha capturado tráfico de red como paso previo a su ataque.	15	Práctica (50%) FEM (50%)
2.d) Se ha accedido a redes inalámbricas vulnerables.	20	Práctica
2.e) Se han caracterizado otros sistemas de comunicación inalámbricos y sus vulnerabilidades.	25	Examen teórico
2.f) Se han utilizado técnicas de “Equipo Rojo y Azul”.	15	Práctica
2.g) Se han realizado informes sobre las vulnerabilidades detectadas.	10	Práctica (50%) FEM (50%)

Recursos

Aula-taller con ordenadores para cada uno de los alumnos de la clase.

Los equipos deberán contar con herramientas de ofimática básicas, software de virtualización y suficiente memoria y disco duro como para poder virtualizar varias máquinas de forma rápida.

Una pantalla o proyector.

Será necesario también contar con equipos que incluyan tarjetas de red configurables en modo monitor o tarjetas externas que lo permitan, así como un punto de acceso.

Se emplearán tarjetas RFID por lo que harán falta lectores/grabadores.

Observaciones

Unidad de Aprendizaje Nº 5 Hacking, todo lo que sabemos y no sabemos.		
Temporalización: Semana 21ª- 30ª	**Duración**: 36h	**Ponderación**:30 %

Objetivos Generales	Competencias
ñ) Combinar técnicas de hacking ético interno y externo para detectar vulnerabilidades que permitan eliminar y mitigar los riesgos asociados. q) Desarrollar manuales de información utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa. r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de	i) Detectar vulnerabilidades en sistemas, redes y aplicaciones, evaluando los riesgos asociados. k) Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente respondiendo a los requisitos establecidos. l) Adaptarse a las nuevas situaciones laborales manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los

la información y la comunicación para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales. s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal. t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo para garantizar entornos seguros. u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas». v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje para valorar la	recursos existentes en el aprendizaje a lo largo de la vida. m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo. n) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización. ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.

cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.	

Resultados de Aprendizaje
1. Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético. **2. Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades.** **3. Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.** **4. Consolida y utiliza sistemas comprometidos garantizando accesos futuros.** **5. Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas.**

Aspectos del Saber Hacer	Aspectos del Saber
Conoce los procedimientos y las etapas que tiene el proceso de hacking. Documenta las vulnerabilidades encontradas en un sistema. Conoce las diferentes técnicas de penetración que existen. Caracteriza y documenta los diferentes tipos de vulnerabilidades.	Fases del hacking. Documentación de vulnerabilidades. Clasificación de herramientas de seguridad y hacking. Documentación de vulnerabilidades. Clasificación de herramientas de seguridad y hacking. Modo infraestructura, ad-hoc y monitor.

Clasifica herramientas de monitorización, seguridad y hacking en base a las necesidades. Configura la tarjeta de red del equipo en sus diferentes modos de funcionamiento. Conoce el funcionamiento de la criptografía en las redes inalámbricas y los estándares que se utilizan en la actualidad de forma comercial. Captura e intercepta paquetes de datos en redes inalámbricas. Vulnera un punto de acceso inalámbrico Conoce otras tecnologías de red inalámbricas, sus topologías posibles, sus vulnerabiliades y usos más habituales. Sabe trabajar con la técnica de "Equipo rojo equipo azul" probar la seguridad de un entorno. Elabora informes de auditoría sobre las vulnerabiliadades detectadas en un entorno.	Comunicación inalámbrica. 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. Realización de informes de auditoría y presentación de resultados. Fase de reconocimiento (*footprinting*). Herramientas de búsqueda y explotación de vulnerabilidades. Ingeniería social. *Phising*. Fase de escaneo (*fingerprinting*). Monitorizacion de tráfico. Interceptación de comunicaciones utilizando distintas técnicas. Manipulación e inyección de tráfico.

Recopila información de la red a partir de datos de fuentes abiertas. Realiza un análisis activo de información de la red como equipos, direcciones, usuarios... Intercepta el tráfico web para descubrir información sobre la red y los sistemas que están en ella. Realiza un ataque de tipo *man in the middle* modificando el tráfico web entre dos máquinas. Vulnera un sistema remoto adquiriendo acceso a nivel usuario y privilegiado dentro de una máquina. Administra sistemas en remoto empleando diferentes tipos de consolas. Utiliza software especializado en ataques a contraseñas para vulnerarlas. Vulnera sistemas no objetivo para acceder a máquinas que contienen la información deseada utilizando	Escalada de privilegios. 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). Negación de credenciales en aplicaciones web. Automatización de conexiones a servidores web (ejemplo: Selenium). Recolección de información Análisis de tráfico a través de proxies de intercepción. Búsqueda de vulnerabilidades habituales en aplicaciones web. Herramientas para la explotación de vulnerabilidades web. Herramientas para la explotación de vulnerabilidades web.

técnicas de pivoting o de pass the hash. Compromete sistemas de manera que se puede garantizar su acceso posteriormente. Conoce y vulnera diferentes tipos de sistemas de autenticación web. Usa técnicas de enumeración para conocer la arquitectura del backend de la aplicación web. Implementa proxies para capturar el tráfico entre el ordenador y el servidor Detecta vulnerabilidades web habituales analizándo el código y el comportamiento de la misma. Automatiza la obtención de vulnerabilidades de una web mediante el uso de scripts y herramientas dedicadas. Explota vulnerabilidades web.	
Aspectos del Saber Estar	

Valora la importancia de la seguridad de las redes inalámbricas y de usar una tecnología segura en las mismas. Identifica la técnica más adecuada para cada tipo de clave. Valora el seguimiento de procedimientos a la hora de atacar redes. Valora el seguimiento de procedimientos a la hora de atacar redes. Evalua el comportamiento de las aplicaciones web mediante su comportamiento a través de proxies.	

Tareas y Actividades

- Se realizarán prácticas que combinan todas las técnicas impartidas a lo largo del curso. Se plantea el uso de HTB o HackMyVM.

Criterios de Evaluación	%	IE
1.e) Se han identificado las fases de un ataque seguidas por un atacante.	10	Autoevaluación
1.f) Se han analizado y definido los tipos vulnerabilidades.	10	Autoevaluación
1.g) Se han analizado y definido los tipos de ataque	10	Autoevaluación

1.h) Se han determinado y caracterizado las diferentes vulnerabilidades existentes.	10	Autoevaluación (50%) FEM (50%)
1.i) Se han determinado las herramientas de monitorización disponibles en el mercado adecuadas en función del tipo de organización.	10	Autoevaluación
2.a) Se han configurado los distintos modos de funcionamiento de las tarjetas de red inalámbricas.	5	Práctica
2.b) Se han descrito las técnicas de encriptación de las redes inalámbricas y sus puntos vulnerables.	10	Examen teórico
2.c) Se han detectado redes inalámbricas y se ha capturado tráfico de red como paso previo a su ataque.	15	Práctica (50%) FEM (50%)
2.d) Se ha accedido a redes inalámbricas vulnerables.	20	Práctica
2.e) Se han caracterizado otros sistemas de comunicación inalámbricos y sus vulnerabilidades.	25	Examen teórico
2.f) Se han utilizado técnicas de “Equipo Rojo y Azul”.	15	Práctica
2.g) Se han realizado informes sobre las vulnerabilidades detectadas.	10	Práctica (50%) FEM (50%)
3.a) Se ha recopilado información sobre la red y sistemas objetivo mediante técnicas pasivas.	20	Práctica (50%) FEM (50%)
3.b) Se ha creado un inventario de equipos, cuentas de usuario y potenciales vulnerabilidades de la red y sistemas objetivo mediante técnicas activas.	20	Práctica
3.c) Se ha interceptado tráfico de red de terceros para buscar información sensible.	20	Práctica
3.d) Se ha realizado un ataque de intermediario, leyendo, insertando y modificando, a voluntad, el tráfico intercambiado por dos extremos remotos.	20	Práctica

3.e) Se han comprometido sistemas remotos explotando sus vulnerabilidades.	20	Práctica
4.a) Se han administrado sistemas remotos a través de herramientas de línea de comandos.	25	Práctica (50%) FEM (50%)
4.b) Se han comprometido contraseñas a través de ataques de diccionario, tablas rainbow y fuerza bruta contra sus versiones encriptadas.	25	Práctica
4.c) Se ha accedido a sistemas adicionales a través de sistemas comprometidos.	25	Práctica
4.d) Se han instalado puertas traseras para garantizar accesos futuros a los sistemas comprometidos.	25	Práctica
5.a) Se han identificado los distintos sistemas de autenticación web, destacando sus debilidades y fortalezas	20	Trabajo individual (50%) FEM (50%)
5.b) Se ha realizado un inventario de equipos, protocolos, servicios y sistemas operativos que proporcionan el servicio de una aplicación web.	20	Práctica (50%) FEM (50%)
5.c) Se ha analizado el flujo de las interacciones realizadas entre el navegador y la aplicación web durante su uso normal.	15	Práctica
5.d) Se han examinado manualmente aplicaciones web en busca de las vulnerabilidades más habituales.	15	Práctica
5.e) Se han usado herramientas de búsquedas y explotación de vulnerabilidades web.	15	Práctica
5.f) Se ha realizado la búsqueda y explotación de vulnerabilidades web mediante herramientas software.	15	Práctica
Recursos		
Aula-taller con ordenadores para cada uno de los alumnos de la clase.		

Los equipos deberán contar con herramientas de ofimática básicas, software de virtualización y suficiente memoria y disco duro como para poder virtualizar varias máquinas de forma rápida. Una pantalla o proyector. Será necesario también contar con equipos que incluyan tarjetas de red configurables en modo monitor o tarjetas externas que lo permitan, así como un punto de acceso. Se emplearán tarjetas RFID por lo que harán falta lectores/grabadores.
Observaciones