Guia docente				
Datos Identificativos				2023/24
Asignatura (*)	Fortificación de Sistemas Operativos		Código	614530108
Titulación	Máster Universitario en Ciberseguridade			
Descriptores				
Ciclo	Periodo	Curso	Tipo	Créditos
Máster Oficial	2º cuatrimestre	Primero	Obligatoria	5
Idioma	CastellanoGallegoInglés			
Modalidad docente	Presencial			
Prerrequisitos				
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónComputación			
Coordinador/a	Yañez Izquierdo, Antonio Fermin	Correo electrónico	antonio.yanez@udc.es	
Profesorado	Yañez Izquierdo, Antonio Fermin	Correo electrónico	antonio.yanez@udc.es	
Web	faitic.uvigo.es			
Descripción general	Un sistema operativo recien instalado es inherentemente inseguro. Presenta ciertas vulnerabilidades dependiendo de factores tales como la edad del S.O., la existencia de puertas traseras sin parchear, los servicios que proporciona y el uso de politicas por defecto que no tienen como primer objetivo la seguridad. Por fortificación de un S.O nos referimos al acto de configurar dicho S.O con la intencion de hacerlo tan seguro como sea posible, intentando minimizar el riesgo de que quede comprometido a ser explotada alguna de sus vulnerabilidades. Esto suele implicar la aplicación de parches de seguridad, el cambio de ciertas políticas por defecto del S.O. y la eliminación (o deshabilitacion) de aplicaciones y servicios no esenciales. En este curso trataremos de identificar vulnerabilidades comunes y ver como el S.O. se puede defender de ellas. Se considerarán sistemas tipo Windows y tipo linux			

Competencias del título	
Código	Competencias del título
A28	HD-08 - Identificar las vulnerabilidades de un SO en un entorno de uso concreto, modificar la configuración mara minimizar su exposición y comprobar su niel de seguridad
B24	K-08 - Distinguir los distintos tipos de vulnerabilidades de los SO, su funcionamiento y configuración, así como la forma que limitan la exposición del SO
C11	C-06 - Identificar vulnerabilidades en un sistema real, así como variar sus parámetros y configurarlo para su protección frente a ellas; limitando así la exposición a amenazas conocidas
C15	C-10 - Diseñar y gestionar la seguridad de infraestructuras para realizar la auditoría de seguridad de la infraestructura y garantizar continuidad de negocio bajo normas y estándares de referencia

Resultados de aprendizaje			
Resultados de aprendizaje	Competencias del título		
Identificar las diferentes vulnerabilidades de un S.O.	AP28		
Entender como funcionan las vulnerabilidades y como el S.O. puede protegerse de ellas		BP24	
Configurar un S.O. de manera que limitemos su exposición a amenazas, minimizando el riesgo de que se vea comprometido			CP11 CP15

Contenidos	
Tema	Subtema
Introducción a F.S.O.	Concepto de fortificación de un S.O. Vulnerabilidades. Fortificación durante la instalación, post instalación y mantenimiento

Fortificación del proceso de arranque	Seguridad física del sistema. Fortificación del firmware (BIOS, UEFI). Fortificación del cargador
Fortificación de las cuentas de usuarios	Identificar y eliminar cuentas no suadas. Limitar privilegios de los usuarios. politicas de grupo. Fortificar autentificación. Forzar políticas de contraseñas
Fortificación de sistemas de ficheros	Permisos y protecciones de sistemas de ficheros. Cuotas. Bloqueo de directorios del sistema. Encriptación. Limitar acceso a dispositivos
Fortificación de aplicaciones	Identificando y eliminando aplicaciones no usadas. Identificando conexiones y aplicaciones que proporcionan conexiones no deseadas. Ejecución en entornos seguros (tipo contenedor), SELinux
Fortificacion de la red	Identificar y eliminar conexiones no deseadas. Filtrado de paquetes
Monitorización y mantenimiento	Monitorización del sistema. Logs. Parches

Planificación				
Metodologías / pruebas	Competéncias	Horas presenciales	Horas no presenciales / trabajo autónomo	Horas totales
Sesión magistral	A28 B24 C11 C15	16	32	48
Prácticas de laboratorio	A28 B24 C11 C15	26	0	26
Prueba práctica	A28 B24 C11	4	14	18
Prueba objetiva	A28 B24 C11	3	30	33
Atención personalizada		0	0	0
(*)Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos				

Metodologías	
Metodologías	Descripción
Sesión magistral	El estudiante asistirá las sesiones magistrales impartidas por el profesor sobre como minimizar la posibilidad de que las distintas vulnerabilidades (arranque, usuarios, conexiones de red..) puedan ser aprovechadas para comprometer el S.O..
Prácticas de laboratorio	Practicas de laboratorio sobre la fortificación de sistemas operativos reales. Se considerarán tanto sistemas Windows como Linux
Prueba práctica	Resolver problemas similares a los realizados en las prácticas sobre una máquina física (real o virtualizada) con la única ayuda de la documentación disponible en la propia máquina.
Prueba objetiva	Test ssobre los contenidos fundamentales de la asignatura.

Atención personalizada	
Metodologías	Descripción
Sesión magistral Prueba práctica Prueba objetiva Prácticas de laboratorio	Si bien las prácticas de laboratorio y la resolución de problemas se realizarán en su mayor parte en horario de clase, el profesor estará disponible para ayudar individualmente con cualquier duda que surja de la realización de estas tareas. El profesor estará disponible para ayudar con los conceptos expuestos durante las sesiones magistrales. Horarios de tutorías UDC Atópanse aquí Los horarios de tutorías de la udc se encuentran aquí https://www.udc.es/es/centros_departamentos_servizos/centros/titorias/?codigo=614

Evaluación			
Metodologías	Competéncias	Descripción	**Calificación**

Prueba práctica	A28 B24 C11	También habrá una prueba práctica donde el alumno realizará unos ejercicios en un ordenador físico (máquina real o virtualizada) sin ayuda de material adicional. Esta prueba se realizará en las sesiones de prácticas, después de cada parte de prácticas (linux y windows). Representa el 40% de la nota de la asignatura (20% la parte Linux y 20% la parte Windows). Los alumnos no presenciales que deseen realizar evaluación contínua deberán realizar estas pruebas, que en este caso representan un 60% (30% para Linux y 30% para Windows)	40
Prueba objetiva	A28 B24 C11	Questiones realacionadas con el conocimiento adquirido Questiones que impliquen razonar sobre el conocimiento adquirido Questiones que involucran resolucion de problemas en Sistemas Operativos reales Para superar la asignatura es necesario superar ambas partes por separado: prueba objetiva y prácticas de laboratorio El valor de esta prueba es del 40%	40
Prácticas de laboratorio	A28 B24 C11 C15	Control de las prácticas realizadas y evaluación de los resultados obtenidos: Las prácticas realizadas durante las sesiones prácticas se evaluarán un 20% de la asignatura (10% para Linux y 10% para Windows)	20

Observaciones evaluación
En las oportunidades ordinarias y extraordinarias sólo se hará la prueba objetiva. Los alumnos que opten por no participar en la evaluación continua y decidan realizar la evaluación global deberán realizar una prueba ese mismo día que valdrá el 100% de la nota de la asignatura. Esta prueba consistirá en una prueba objetiva, una prueba práctica o una combinación de ambas. Para renunciar a la evaluación continua y acogerse a la evaluación global, se debe enviar un correo electrónico a antonio.yanez@udc.esmiyolanda@det.uvigo.es antes de una semana de la fecha de la oportunidad ordinaria o, en su caso, extraordinaria.

Fuentes de información

Básica	- Donald A. Tevault (2018). Mastering Linux Security and Hardening. Packt Publishing - James Turnbull (2008). Hardening Linux . Apress - Carlos Álvarez Martín y Pablo González Pérez 0xWord (2016). Hardening de servidores GNU / Linux (3a Edicion). 0xWord - Tajinder Kalsi (2018). Practical Linux Security Cookbook: Secure your Linux environment from modern-day attacks with practical recipes, 2nd Edition. Packt Publishing - Yuri Diogenes, Erdal Ozkaya (2018). Cybersecurity - Attack and Defense Strategies. Packt Publishing - Gris, Myriam (2017). Windows 10. ENI - Aprea, Jean-François (2017). Windows Server 2016 : Arquitectura y Administración de los servicios de dominio Active Directory. ENI - Bonnet, Nicolas (2017). Windows Server 2016 : las bases imprescindibles para administrar y configurar su servido. ENI - De los Santos, Sergio (). Máxima Seguridad en Windows: Secretos Técnico. 0xWord - Núñez, Ángel (). Windows Server 2016: Administración, seguridad y operaciones. 0xWord - Salvy, Pierre (2017). Windows 10 : despliegue y gestión a través de los servicios de empresa. ENI - Deman, Thierry (2018). Windows Server 2016 : Administración avanzada. ENI - García, Carlos. González, Pablo (). Hacking Windows: Ataques a sistemas y redes Microsoft. 0xWord
Complementária	

Recomendaciones
Asignaturas que se recomienda haber cursado previamente
Asignaturas que se recomienda cursar simultáneamente
Asignaturas que continúan el temario
Otros comentarios

(*) La Guía Docente es el documento donde se visualiza la propuesta académica de la UDC. Este documento es público y no se puede modificar, salvo cosas excepcionales bajo la revisión del órgano competente de acuerdo a la normativa vigente que establece el proceso de elaboración de guías