UNIVERSIDADE DA CORUÑA

Guía Docente				
Datos Identificativos				2022/23
Asignatura (*)	Fortificación de Sistemas Operativos		Código	614530007
Titulación				
Descriptores				
Ciclo	Período	Curso	Tipo	Créditos
Mestrado Oficial	2º cuadrimestre	Primeiro	Obrigatoria	5
Idioma	CastelánGalegoInglés			
Modalidade docente	Presencial			
Prerrequisitos				
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónComputación			
Coordinación	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			
Descrición xeral	Un sistema operativo recentemente instalado é inherentemente inseguro. Presenta certas vulnerabilidades dependendo de factores tales como a idade do S.O., a existencia de portas traseiras sen parchear, os servizos qu eproporciona e o uso de políticas por defecto que non teñen como primeriro obxectivo a seguridade. Por fortificación dun S.O. referímonos ó acto de configurar dito S.O. coa intención de facelo tan seguro como sexa posible, intentanto minimizar o risco de que quede comprometido a ser explotada algunha das vulnerabilidades. Isto xeralmente iimplica a aplicación de parches de seguridade, o cambio de certas políticas por defecto del S.O. e a eliminación (ou deshabilitacion) de aplicacións e servizos non esenciais.			

Competencias / Resultados do título	
Código	Competencias / Resultados do título

Resultados da aprendizaxe			
Resultados de aprendizaxe	Competencias / Resultados do título		
Identificar as diferentes vulnerabilidades dun S.O.		BP2 BP5 BP6 BP7 BP10	
Entender como funcionan as vulnerabilidades e como o S.O. se pode protexer delas	AP8	BP2 BP5 BP6 BP7 BP10	
Configurar un S.O. de xeito que limitemos a súa exposición a amenazas, minimizando o risco de que se vexa comprometido	AP3 AP4 AP5 AP8 AP9 AP11 AP13	BP2 BP5 BP6 BP7 BP8	CP3 CP4

Contidos	
Temas	Subtemas

Introducción á F.S.O.	Concepto de fortificación dun S.O. Vulnerabilidades. Fortificación durante a instalación, post instalación e mantemento
Fortificación do proceso de arranque	Seguridad física del sistema. fortificación do firmware (BIOS, UEFI). Fortificación do cargador
Fortificación das contas de usuario	identificar i eliminar contas non usadas. limitar os privilexios dos usuarios. Políticas de grupo. Fortificar a autenticación. Forzar políticas de contrasinais
Fortificación dos sistemas de ficheiros	Permisos e proteccións de sistemas de ficheiros. Cuotas. Bloqueo de directorios do sistema. Encriptación. Limitar acceso a dispositivos.
Fortificación de aplicaciones	Identificando i eliminando aplicacións non usadas. identificando conexións e aplicacións que proporcionan conexións non desexadas. Execución en entornos seguros (tipo contedor), SELinux
Fortificación de red	Identificar i eliminar conexións non desexadas. Filtrado de paquetes.
Monitorización e mantemento	Monitorización do sistema. Logs. Parches.

Planificación				
Metodoloxías / probas	Competencias / Resultados	Horas lectivas (presenciais e virtuais)	Horas traballo autónomo	Horas totais
Actividades iniciais	A8 A11 A13 B6	1	2	3
Sesión maxistral	A3 A4 A11 A13 B5 B6 B8 B10 C3	16	32	48
Solución de problemas	A3 A4 A5 B2 B5 B7 B8 B10 C3	5	15	20
Prácticas de laboratorio	A4 A5 A8 A9 A11 A13 B2 B5 B6 B7 B8 B10 C3	16	16	32
Proba obxectiva	A3 A4 A5 A8 A9 A11 A13 B2 B5 B6 B7 B8 B10 C3 C4	2	20	22
Atención personalizada		0		0
*Os datos que aparecen na táboa de planificación son de carácter orientativo, considerando a heteroxeneidade do alumnado				

Metodoloxías	
Metodoloxías	Descrición
Actividades iniciais	Actividades iniciais para familiarizar ó alumno co S.O., as súas vulnerabilidades e as defensas frente a elas
Sesión maxistral	O estudante asistirá ás sesións maxistrais impartidas polo profesor sobre como minimizar a posibilidade de que as distintas vulnerabilidades (arranque, usuarios, conexións de rede...) podan ser aproveitadas para comprometer o S.O.
Solución de problemas	Problemas e pequenas cuestións prácticas para conolidar os contidos presentados nas sesións maxistrais
Prácticas de laboratorio	Prácticas de laboratorio sobre a fortificación de sistemas operativos reais. Consideraranse tanto sistemas Windows coma Linux
Proba obxectiva	Test sobre os contidos fundamentais da materia

Atención personalizada	
Metodoloxías	Descrición

Sesión maxistral Solución de problemas Prácticas de laboratorio	Aínda que as prácticas de laboratorio e a solución de problemas realizarase na súa meirande parte no horario de clases, o profesor estará dispoñible para axudar de xeito individual con calquera dúbida ou cuestión que poda xurdir na realización destas tareas. o profesor estará tamén dispoñible para axudar cos conceptos expostos durante as sesións maxistrais. Aunque las prácticas de laboratorio y la solución de problemas se realizará en su mayor parte en el horario de clases, el profesor estará disponible para ayudar de manera individual con cualquier duda o cuestion que surga de la realización de estas tareas. El profesor estará asimismo disponible para ayudar con los conceptos expuestos durante las sesiones magistrales.

Avaliación			
Metodoloxías	**Competencias / Resultados**	**Descrición**	**Cualificación**
Proba obxectiva	A3 A4 A5 A8 A9 A11 A13 B2 B5 B6 B7 B8 B10 C3 C4	Cuestións relacionadas co coñecemento adquirido Cuestións que impliquen razoar sobre o coñecemento adquirido Cuestións que involucran resolución de problemas en Sistemas Operativos reais Para superar a materia é necesario superar ambas partes por separado: proba obxectiva e prácticas de laboratorio	50
Prácticas de laboratorio	A4 A5 A8 A9 A11 A13 B2 B5 B6 B7 B8 B10 C3	Control das prácticas realizadas e avaliación dos resultados obtidos: As prácticas realizadas durante as sesións de prácticas evaluaranse con ata 40-60% da puntuación de prácticas (20-30% do total) Ademáis haberá unha proba práctica onde o alumno realizará algúns exercicios sobre un equipo físico (máquina real ou virtualizada) sen axusa de material adicional. Dita proba realizarase, ben nas últimas sesións de prácticas, ben despois de cada parte de prácticas (linux e windows) ou o mesmo día da proba obxectiva, despois desta, e representa o 60-40% da puntuación de prácticas (30-20% to total) A covocatoria de Xullo, consiste só de proba obxectiva. Se un estudante tamén quere facer a proba práctica, deberá solicitalo por escritoantes dunha semana da data fixada para a proba obxectiva. Para superar a materia é necesario superar ambas partes por separado: proba obxectiva e prácticas de laboratorio.	50

Observacións avaliación
Para superar a materia é necesario superar ambas partes por separado: proba obxectiva e prácticas de laboratorio A covocatoria de Xullo, consiste só de proba obxectiva. Se un estudante tamén quere facer a proba práctica, deberá solicitalo por escritoantes dunha semana da data fixada para a proba obxectiva.

Fontes de información	
Bibliografía 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 - 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 - Yuri Diogenes, Erdal Ozkaya (2018). Cybersecurity - Attack and Defense Strategies. Packt Publishing - 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
Bibliografía complementaria	

Recomendacións
Materias que se recomenda ter cursado previamente
Materias que se recomenda cursar simultaneamente
Materias que continúan o temario
Observacións

(*)A Guía docente é o documento onde se visualiza a proposta académica da UDC. Este documento é público e non se pode modificar, salvo casos excepcionais baixo a revisión do órgano competente dacordo coa normativa vixente que establece o proceso de elaboración de guías