UNIVERSIDADE DA CORUÑA

Guía Docente				
Datos Identificativos				2023/24
Asignatura (*)	Fortificación de Sistemas Operativos		Código	614530108
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 primeiro 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 e sexa explotada algunha das vulnerabilidades. Isto xeralmente iimplica a aplicación de parches de seguridade, o cambio de certas políticas por defecto do 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.	AP28		
Entender como funcionan as vulnerabilidades e como o S.O. se pode protexer delas		BP24	
Configurar un S.O. de xeito que limitemos a súa exposición a amenazas, minimizando o risco de que se vexa comprometido			CP11 CP15

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 e eliminando aplicacións non usadas. identificando conexións e aplicacións que proporcionan conexións non desexadas. Execución en entornos seguros (tipo contedor), Apparmor.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
Sesión maxistral	A28 B24 C11 C15	16	32	48
Prácticas de laboratorio	A28 B24 C11 C15	26	0	26
Proba práctica	A28 B24 C11	4	14	18
Proba obxectiva	A28 B24 C11	3	30	33
Atención personalizada		0	0	0
*Os datos que aparecen na táboa de planificación son de carácter orientativo, considerando a heteroxeneidade do alumnado				

Metodoloxías	
Metodoloxías	Descrición
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.
Prácticas de laboratorio	Prácticas de laboratorio sobre a fortificación de sistemas operativos reais. Consideraranse tanto sistemas Windows coma Linux
Proba práctica	Resolución de problemas similares aos realizados en prácticas nunha máquina física (real ou virtualizada) coa única axuda da documentación dispoñible na propia máquina.
Proba obxectiva	Test sobre os contidos fundamentais da materia

Atención personalizada	
Metodoloxías	Descrición
Sesión maxistral Proba práctica Proba obxectiva Prácticas de laboratorio	Aínda que as prácticas de laboratorio e a solución de problemas realizarase na súa maior 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. Os horarios de tutorias da udc atópanse aqui https://www.udc.es/es/centros_departamentos_servizos/centros/titorias/?codigo=614

Avaliación			
Metodoloxías	Competencias / Resultados	Descrición	**Cualificación**

Proba práctica	A28 B24 C11	Ademáis haberá unha proba práctica onde o alumno realizará algúns exercicios sobre un equipo físico (máquina real ou virtualizada) sen axuda de material adicional. Dita proba realizarase nas sesións de prácticas, despois de cada parte de prácticas (linux e windows). Representa o 40% da puntuación da asignatura (20% a parte de linux e 20% a parte de windows). Os alumnos non presenciais que queran ter evaluación contínua deberán presentarse a estas probas, ainda que para eles representaran o 60% (30% a parte de linux e 30% windows a parte de windows)	40
Proba obxectiva	A28 B24 C11	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 O valor de esta proba é dun 40% da asignatura.	40
Prácticas de laboratorio	A28 B24 C11 C15	Control das prácticas realizadas e avaliación dos resultados obtidos: As prácticas realizadas durante as sesións de prácticas contarán 20% da asignatura (10% a parte de linux e 10% a de windows)	20

Observacións avaliación
Nas oportunidades ordinaria e extraordinaria farase so a proba obxectiva.Os alumnos que renuncien á evaluación continua e se decidan acollerse á global, terán que realizar eses mismos días (oportunidade ordinaria e extraordinaria) una proba que terá un valor do 100% da cualificación da asignatura.Dita proba consistirá nunha proba obxectiva, unha proba práctica ou unha combinación de ambas.Para renunciar a avaliación continua e acollerse a avaliación global deberá enviarse un correo aantonio.yanez@udc.eseyolanda@det.uvigo.esantes dunha semana da data da oportunidade ordinaria ou, no seu caso, extraordinaria.

Fontes de información

UNIVERSIDADE DA CORUÑA

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 - 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
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