



| Guía Docente          |   |                    |                      |           |
|-----------------------|---|--------------------|----------------------|-----------|
| Datos Identificativos |   |                    |                      | 2024/25   |
| Asignatura (*)        | Fortificación de Sistemas Operativos  |                    | Código               | 614530108 |
| Titulación            | Máster Universitario en Ciberseguridad  |                    |                      |           |
| Descriptores          |   |                    |                      |           |
| Ciclo                 | Período   | Curso              | Tipo                 | Créditos  |
| Mestrado Oficial      | 2º cuatrimestre   | 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   |                    |                      |           |
| Descripción xeral     | <p>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.</p> <p>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 implica a aplicación de parches de seguridade, o cambio de certas políticas por defecto do S.O. e a eliminación (ou deshabilitacion) de aplicacóns e servizos non esenciais.</p> |                    |                      |           |

| Competencias / Resultados do título |  |
|-------------------------------------|--|
| Código                              | Competencias / Resultados do título  |
| A28                                 | HD-08 - Identificar las vulnerabilidades de un SO en un entorno de uso concreto, modificar la configuración para minimizar su exposición y comprobar su nivel 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 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<br>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 | Seguridade física do sistema. fortificación do firmware (BIOS, UEFI). Fortificación do cargador   |
| Fortificación das contas de usuario  | identificar e 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 aplicaciones non usadas. identificando conexions e aplicacións que proporcionan conexions non desexadas. Execución en entornos seguros (tipo contedor), Apparmor.SELinux |
| Fortificación de red                    | Identificar e eliminar conexions 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             | Descripción   |
| Sesión maxistral         | O estudiante 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 disponible na propia máquina.  |
| Proba obxectiva          | Test sobre os contidos fundamentais da materia  |

| Atención personalizada  |  |
|---|--|
| Metodoloxías  | Descripción  |
| Sesión maxistral<br>Proba práctica<br>Proba obxectiva<br>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.<br><br>o profesor estará tamén dispoñible para axudar cos conceptos expostos durante as sesións maxistrais.<br><br>Os horarios de tutorias da udc atópanse aquí<br><br><a href="https://www.udc.es/es/centros_departamentos_servicios/centros/tutorias/?codigo=614">https://www.udc.es/es/centros_departamentos_servicios/centros/tutorias/?codigo=614</a> |

| Avaliación   |                           |             |               |
|--------------|---------------------------|-------------|---------------|
| Metodoloxías | Competencias / Resultados | Descripción | Cualificación |



|                          |                 |   |    |
|--------------------------|-----------------|---|----|
| Proba práctica           | A28 B24 C11     | <p>Ademáis haberá unha proba práctica onde o alumno realizará algúns exercicios sobre un equipo físico (máquina real ou virtualizada) sen axuda de material adicional.</p> <p>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).</p> <p>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)</p> | 40 |
| Proba obxectiva          | A28 B24 C11     | <p>Cuestións relacionadas co coñecemento adquirido</p> <p>Cuestións que impliquen razoar sobre o coñecemento adquirido</p> <p>Cuestións que involucran resolución de problemas en Sistemas Operativos reais</p> <p>Para superar a materia é necesario superar ambas partes por separado: proba obxectiva e prácticas de laboratorio</p> <p>O valor de esta proba é dun 40% da asignatura.</p>   | 40 |
| Prácticas de laboratorio | A28 B24 C11 C15 | <p>Control das prácticas realizadas e avaliación dos resultados obtidos:</p> <p>As prácticas realizadas durante as sesións de prácticas contarán 20% da asignatura (10% a parte de linux e 10% a de windows)</p>  | 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 esos 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.es yolanda@det.uvigo.es antes dunha semana da data da oportunidade ordinaria ou, no seu caso, extraordinaria.Todos os aspectos relacionados con ?dispensa académica?, ?dedicación ao estudo?, ?permanencia? e ?fraude académica? rexeranse de acordo coa normativa académica vixente da UDC

#### Fontes de información



|                             |   |
|-----------------------------|---|
| Bibliografía básica         | <ul style="list-style-type: none"><li>- Donald A. Tevault (2018). Mastering Linux Security and Hardening. Packt Publishing</li><li>- James Turnbull (2008). Hardening Linux . Apress</li><li>- Carlos Álvarez Martín y Pablo González Pérez 0xWord (2016). Hardening de servidores GNU / Linux (3a Edicion). 0xWord</li><li>- Tajinder Kalsi (2018). Practical Linux Security Cookbook: Secure your Linux environment from modern-day attacks with practical recipes, 2nd Edition. Packt Publishing</li><li>- Yuri Diogenes, Erdal Ozkaya (2018). Cybersecurity - Attack and Defense Strategies. Packt Publishing</li><li>- Gris, Myriam (2017). Windows 10. ENI</li><li>- Aprea, Jean-François (2017). Windows Server 2016 : Arquitectura y Administración de los servicios de dominio Active Directory. ENI</li><li>- Bonnet, Nicolas (2017). Windows Server 2016 : las bases imprescindibles para administrar y configurar su servido. ENI</li><li>- De los Santos, Sergio (). Máxima Seguridad en Windows: Secretos Técnico. 0xWord</li><li>- Núñez, Ángel (). Windows Server 2016: Administración, seguridad y operaciones. 0xWord</li><li>- Salvy, Pierre (2017). Windows 10 : despliegue y gestión a través de los servicios de empresa. ENI</li><li>- Deman, Thierry (2018). Windows Server 2016 : Administración avanzada. ENI</li><li>- García, Carlos. González, Pablo (). Hacking Windows: Ataques a sistemas y redes Microsoft. 0xWord</li></ul> |
| Bibliografía complementaria |   |

#### Recomendacións

Materias que se recomienda ter cursado previamente

Materias que se recomienda 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