GUIA DOCENT

SEGURETAT D'APLICACIONS I COMUNICACIONS

Coordinació: FERNANDEZ CAMON, CESAR

Any acadèmic 2023-24

SEGURETAT D'APLICACIONS I COMUNICACIONS 2023-24

Informació general de l'assignatura

<table>
<tr><td>Denominació</td><td>SEGURETAT D'APLICACIONS I COMUNICACIONS</td></tr>
<tr><td>Codi</td><td>102028</td></tr>
<tr><td>Semestre d'impartició</td><td>1R Q(SEMESTRE) AVALUACIÓ CONTINUADA</td></tr>
<tr><td>Caràcter</td><td>
<table>
<tr><th>Grau/Màster</th><th>Curs</th><th>Caràcter</th><th>Modalitat</th></tr>
<tr><td>Grau en Enginyeria Informàtica</td><td>4</td><td>OBLIGATÒRIA</td><td>Presencial</td></tr>
<tr><td>Grau en Enginyeria Informàtica</td><td>4</td><td>OPTATIVA</td><td>Presencial</td></tr>
</table>
</td></tr>
<tr><td>Nombre de crèdits assignatura (ECTS)</td><td>9</td></tr>
<tr><td>Tipus d'activitat, crèdits i grups</td><td>
<table>
<tr><th>Tipus d'activitat</th><th>PRALAB</th><th>TEORIA</th></tr>
<tr><td>Nombre de crèdits</td><td>4.5</td><td>4.5</td></tr>
<tr><td>Nombre de grups</td><td>1</td><td>1</td></tr>
</table>
</td></tr>
<tr><td>Coordinació</td><td>FERNANDEZ CAMON, CESAR</td></tr>
<tr><td>Departament/s</td><td>ENGINYERIA INFORMÀTICA I DISSENY DIGITAL</td></tr>
<tr><td>Distribució càrrega docent entre la classe presencial i el treball autònom de l'estudiant</td><td>9 ECTS = 25x9 = 225 hores de treball
40% --> 90 hores presencials
60% --> 135 hores de treball autònom</td></tr>
<tr><td>Informació important sobre tractament de dades</td><td>Consulteu aquest enllaç per a més informació.</td></tr>
<tr><td>Idioma/es d'impartició</td><td>Català / Anglés
Materials en anglés.</td></tr>
</table>

SEGURETAT D'APLICACIONS I COMUNICACIONS 2023-24

Professor/a (s/es)	Adreça electrònica professor/a (s/es)	Crèdits impartits pel professorat	Horari de tutoria/lloc
FERNANDEZ CAMON, CESAR	cesar.fernandez@udl.cat	3	
MATEU PIÑOL, CARLOS	carles.mateu@udl.cat	3	
SEBE FEIXAS, FRANCISCO	francesc.sebe@udl.cat	3	

Informació complementària de l'assignatura

Per cursar l'assignatura es requereixen coneixements prèvis de sistemes operatius, programació, xarxes i comunicacions.

Objectius acadèmics de l'assignatura

- Entendre els conceptes, problemes i procediments de seguretat informàtica
- Entendre i ser capaços de fer una anàlisi de riscos senzilla
- El·laborar auditories de seguretat senzilles
- Entendre els conceptes i mecanismes bàsics de la criptografia
- Dissenyar i configurar esquemes de tallafocs

Competències

CT2. Adquirir un domini significatiu d'una llengua estrangera, especialment de l'anglès.

CT3. Adquirir capacitació en l'ús de les noves tecnologies i de les tecnologies de la informació i la comunicació.
Competències específiques de la titulació

GII-TI2. Capacitat per seleccionar, dissenyar, desplegar, integrar, avaluar, construir, gestionar, explotar i mantenir les tecnologies de hardware, software i xarxes, dins dels paràmetres de cost i qualitat adequats.

GII-TI6. Capacitat de concebre sistemes, aplicacions i serveis basats en tecnologies de xarxa, incloent Internet, web, comerç electrònic, multimèdia, serveis interactius i computació mòbil.

GII-TI7. Capacitat per comprendre, aplicar i gestionar la garantia i seguretat dels sistemes informàtics.

EPS11. Capacitat de comprendre les necessitats de l'usuari expressades en un llenguatge no tècnic.

Continguts fonamentals de l'assignatura

SEGURETAT D'APLICACIONS I COMUNICACIONS 2023-24

1. Introducció
2. Preliminars
    1. Conceptes previs
    2. Virtualització (pels laboratoris)
3. Seguretat de sistemes
4. Seguretat d'aplicacions: exploits i vulnerabilitats.
5. Auditories de seguretat.
6. Criptografia
    - Criptografia simètrica
        - Xifratge de bloc
        - Xifratge de flux
    - Funcions Hash
    - Criptografia asimètrica
        - Fonaments matemàtics
        - Xifratge de clau pública RSA
        - Signatura digital RSA
7. Tallafocs
    - Filtratge del tràfic de xarxa
    - Disseny de tallafocs per a estacions de treball, servidors i routers.
8. Autenticació
    - Introducció OpenSSL
    - Gestió de claus
    - Aplicacions d'autenticació
        - kerberos
        - X509
    - Infraestructura de clau pública
9. Comunicacions segures
    - Programant en SSL
    - SMIME
    - DNIe
    - OpenVPN

Eixos metodològics de l'assignatura

Cadascún dels temes que composen l'assignatura es presenta en classes magistrals. En funció dels continguts, es proposa la resolució de problemes pràctics i/o casos pràctics. Tant els problemes com els casos pràctics es desenvolupen en grup, són parcialment tutoritzats a classe i són avaluats.

Pla de desenvolupament de l'assignatura

- Setmana 1,2: Temes 1,2
- Setmana 3,4: Tema 3
- Setmana 5,6: Temes 4 i 5
- Setmana 7-10: Tema 6
- Setmana 11,12: Tema 7
- Setmana 13,14: Tema 8
- Setmana 15,16: Tema 9

Sistema d'avaluació

L'avaluació s'estructura en 6 blocs. Cap d'ells requereix nota mínima i la nota de cada bloc s'obté realitzant exercicis i casos pràctics. La puntuació és la següent:

Bloc 1. Seguretat de sistemes (19)

- Virtualització (5)
- Sistemes bàsics de seguretat (7 + 7)

Bloc 2 Auditoria i aplicacions (15)

- Fallides de programació: stack exploits, etc. (7)
- Auditoria bàsica de seguretat: (8)

Bloc 3. Criptografia (21)

- Criptografia de clau compartida (4+4+4+3)
- Criptografia de clau pública (3+3)

Bloc 4. Sistemes tallafocs (12)

- Tallafocs en una estació de treball (6)
- Tallafocs en un servidor (6)

Bloc 5. Autenticació (16)

- Clau simètrica amb OpenSSL (4)
- Clau pública amb OpenSSL (5)
- Firma digital (3+2)
- Infraestructura de clau pública (2)

Bloc 6. Aplicacions de seguretat (16)

- SSL (4+2)
- SMIME (5)
- DNIe (2)
- OpenVPN (3)

Per aprovar el curs es requereix obtenir més del 50% dels punts.

L'avaluació alternativa de l'assignatura implica el lliurament de les mateixes activitats. En aquest cas, el plaç d'entrega s'amplia fins 3 dies hàbils abans del tancament de les actes.

Bibliografia i recursos d'informació

- Network Security with OpenSSL. Pravir Chandra, Matt Messier, John Viega. Ed. O'Reilly, 2002
- Cryptography & Network Security, W. Stallings, 3-Ed, 2003
- Network & Internetwork Security, W. Stallings, 1995
- Advanced Penetration Testing for Highly-Secured Environments. Lee Allen. Packt Publishing. 2012.
- Threat Modeling. Adam Shostack. Wiley. 2014.
- Metasploit Penetration Testing Cookbook. Abhinav Singh. Pack Publishing. 2012.
- Gray Hat Hacking: The Ethical Hackers Handbook. Harper, Harris et al. McGraw-Hill.2011
- Netfilter project homepage, https://www.netfilter.org/