VNIVERSITAT DE VALÈNCIA

Guia Docent
43861 Seguretat en xarxes

FITXA IDENTIFICATIVA

Dades de l'Assignatura

Codi	43861
Nom	Seguretat en xarxes
Cicle	Màster
Crèdits ECTS	5.0
Curs acadèmic	2022 - 2023

Titulació/titulacions

Titulació	Centre	Curs	Període
2174 - M.U. en Enginyeria de Telecomunicació 13-V.2	Escola Tècnica Superior d'Enginyeria	2	Primer quadrimestre

Matèries

Titulació	Matèria	Caràcter
2174 - M.U. en Enginyeria de Telecomunicació 13-V.2	15 - Seguretat en xarxes	Obligatòria

Coordinació

Nom	Departament
GARCIA PINEDA, MIGUEL	240 - Informàtica

RESUM

Aquesta assignatura se centra en l'estudi, des d'un punt de vista tant teòric com pràctic, dels diferents mecanismes i eines existents en l'actualitat per garantir la seguretat d'una intranet corporativa, tant davant d'atacs exteriors com interiors, tant per la xarxa cablejada com per a la xarxa sense fils.
L'assignatura prepara l'alumne per certificacions oficials relacionades amb la seguretat que posseeixen una gran demanda professional en el sector de les telecomunicacions. La certificació obri les portes a un sector estratègic com és Internet en el món empresarial i de negocis.
L'assignatura s'ha dissenyat seguint una metodologia adaptada al nou Espai Europeu d'Educació Superior (EEES), i pretén centrar l'aprenentatge en l'estudiant. Aquest mètode millora la implicació de l'estudiant i ajuda a la seva avaluació de forma contínua, reforçant i complementant els coneixements adquirits en classes magistrals.

CONEIXEMENTS PREVIS

Relació amb altres assignatures de la mateixa titulació

No heu especificat les restriccions de matrícula amb altres assignatures del pla d'estudis.

Altres tipus de requisits

Ser capaç de manejar els comandaments de xarxa de Linux i de Windows, així com entendre els fonaments d'IP, TCP / IP, UDP / IP, DHCP, punts d'accés i routers necessaris per configurar una petita LAN.

COMPETÈNCIES

2174 - M.U. en Enginyeria de Telecomunicació 13-V.2

- Capacitat d'anàlisi i pensament crític, per investigar amb independència i autocrítica, i de buscar i utilitzar informació per documentar idees.
- Que els estudiants sàpiguen aplicar els coneixements adquirits i la seua capacitat de resolució de problemes en entorns nous o poc coneguts dins de contextos més amplis (o multidisciplinaris) relacionats amb la seua àrea d?estudi.
- Que els estudiants posseïsquen les habilitats d?aprenentatge que els permeten continuar estudiant d?una forma que haurà de ser en gran manera autodirigida o autònoma.
- Posseir i comprendre coneixements que aportin una base o oportunitat de ser originals en el desenvolupament i / o aplicació d'idees, sovint en un context de recerca.
- Ser capaços d'accedir a ferramentes d'informació en altres àrees del coneixement i utilitzar-les apropiadament.
- Ser capaços de valorar la necessitat de completar la seva formació científica, històrica, en llengües, en informàtica, en literatura, en ètica, social i humana en general, assistint a conferències o cursos i / o realitzant activitats complementàries, autoavaluant l'aportació que la realització d'aquestes activitats suposa per a la seva formació integral.
- Capacitat per a modelar, dissenyar, implantar, gestionar, operar, administrar i mantindre xarxes, servicis i continguts.
- Capacitat per a realitzar la planificació, presa de decisions i empaquetatge de xarxes, servicis i aplicacions considerant la qualitat de servici, els costos directes i d'operació, el pla d'implantació, supervisió, els procediments de seguretat, l'escalat i el manteniment, així com gestionar i assegurar la qualitat en el procés de desenrotllament.
- Capacitat de comprendre i saber aplicar el funcionament i organització d'Internet, les tecnologies i protocols d'Internet de nova generació, els models de components, programari intermediari i servicis.

RESULTATS DE L'APRENENTATGE

Una vegada finalitzat el curs, l'alumne haurà adquirit els coneixements per a:

- Descriure els conceptes comuns de seguretat de xarxa

- Assegurar una infraestructura de routing i switching

- Desenvolupar serveis d'autenticació bàsica, autorització i auditoria

- Desenvolupar serveis bàsics de tallafocs

- Desplegament bàsic de punt a punt i els serveis d'accés remot VPN

- Descriure l'ús dels serveis de seguretat més avançades, com ara la protecció d'intrusos, seguretat de contingut i gestió d'identitats

DESCRIPCIÓ DE CONTINGUTS

1. Amenaces de seguretat en les xarxes

1.1. Principis fonamentals de les xarxes segures
1.2. Cucs, virus i troians
1.3. Metodologies d'atac

2. Assegurar els dispositius de xarxa

2.1. Assegurar l'accés i els fitxers dels dispositius
2.2. CLI basada en rols
2.3. Dispositius de monitorització
2.4. Utilització de característiques automatitzades

3. Autenticació, autorització i auditoria

3.1. Propòsit d'AAA
3.2. Configuració local d'AAA
3.3. Configuració d'AAA basada en servidor

4. Implementació de tecnologies de tallafocs

4.1. Llistes de control d'accés
4.2. Tecnologies de tallafocs
4.3. Control d'accés basat en context
4.4. Polítiques de tallafocs

5. Implementació de la prevenció de la intrusió

5.1. tecnologies IPS
5.2. Implementació d'IPS

6. Assegurant la xarxa d'àrea local

6.1 Consideracions finals de seguretat
6.2. Consideracions de seguretat de capa 2
6.3. Wireless, VoIP i consideracions de seguretat SAN
6.4. Configuració de la seguretat del switch
6.5. SPAN i RSPAN

7. Criptografia

7.1. serveis criptogràfics
7.2. Resums, signatures digitals i autenticació
7.3. Encriptació simètrica i asimètrica

8. Implementació de les xarxes privades virtuals

8.1. VPNs
8.2. Components i operacions de les VPNs IPSEC
8.3. Implementació de VPNs site-to-site.
8.4. Implementació de VPNs d'accés remot
8.5. Implementació de SSLVPNs

9. Gestionar una xarxa segura

9.1. Cicle de vida d'una xarxa segura
9.2. Xarxa d'autodefensa
9.3. Construcció d'una política integral de seguretat

VOLUM DE TREBALL

ACTIVITAT	Hores	% Presencial
Classes de teoria	21,00	100
Pràctiques en aula	18,00	100
Pràctiques en laboratori	9,00	100
Tutories reglades	2,00	100
Elaboració de treballs individuals	30,00	0
Estudi i treball autònom	30,00	0
Preparació d'activitats d'avaluació	5,00	0
Preparació de classes de teoria	5,00	0
Preparació de classes pràctiques i de problemes	5,00	0
TOTAL	**125,00**	

METODOLOGIA DOCENT

Les activitats formatives es desenvoluparan d'acord amb la següent distribució:

El 40% de les hores dels crèdits ECTS (1 crèdit són 25 hores) es destinaran a les següents

activitats presencials:

MD1.- Activitats teòriques.

- Descripció: A les classes teòriques es desenvoluparan els temes proporcionant una visió global i integradora, analitzant amb major detall els aspectes clau i de major complexitat, fomentant, en tot moment, la participació del / la estudiant.

MD2.- Activitats pràctiques.

- Descripció: Complementen les activitats teòriques amb l'objectiu d'aplicar els conceptes bàsics i ampliar-los amb el coneixement i l'experiència que vagin adquirint durant la realització dels treballs proposats. Comprenen els següents tipus d'activitats presencials: Classes de problemes i qüestions en aula; sessions de discussió i resolució de problemes i exercicis prèviament treballats pels estudiants; pràctiques de laboratori; presentacions orals; conferències; tutories programades (individualitzades o en grup)

Avaluació.

- Descripció: Realització de qüestionaris individuals d'avaluació en l'aula amb la presència del professorat.

El 60% de les hores dels ECTS (25 hores per ECTS) es dedicaran a les següents activitats no presencials:

Treball personal de l'estudiant / a.

- Descripció: Realització (fora de l'aula) de treballs monogràfics, recerca bibliogràfica dirigida, qüestions i problemes, així com la preparació de classes i exàmens (estudi). Aquesta tasca es realitzarà de manera individual i intenta potenciar el treball autònom.

S'utilitzarà la plataforma d'e-learning (Aula Virtual) de la Universitat de València com a suport de comunicació amb els estudiants. A través d'ella es tindrà accés al material didàctic utilitzat en classe, així com els problemes i exercicis a resoldre

AVALUACIÓ

L'assignatura s'avaluarà de la següent manera en avaluació contínua:

1. SE1:- Part teòrica examen final (35%). Nota mínima 5. Com a alternativa en avaluació contínua es realitzaran exàmens escrits mitjanats.

2. SE2.- Part laboratori (50%)

1. Assistència, preparació i realització de la pràctica avaluada en el mateix laboratori (10%).
2. Examen escrit de configuració amb ordres (40%). Nota mínima 5. Com a alternativa es realitzaran exàmens pràctics mitjanats.

3. SE3.- Exercicis proposats pel professor (15%).

En segona convocatòria, s'aplicarà el mateix que en la primera.

En qualsevol cas, el sistema d'avaluació es regirà per l'establert en el Reglament d'Avaluació i Qualificació de la Universitat de València per a Graus i Màsters.(http://www.uv.es/graus/normatives/2017_108_Reglament_avaluacio_qualificacio.pdf).

REFERÈNCIES

Bàsiques

- Stallings, Network Security Essential (5th edition), 2013
- Mark Rhodes-Ousley, Roberta Bragg, Keith Strassberg. Network Security: The Complete Reference
- Cisco Press: Designing Network Security
- Omar Santos, John Stuppi. CCNA Security 210-260 Official Cert Guide. Cisco Press, 2015