Pla docent de *Estratègies de Seguretat en Xarxes i Serveis*

Pla docent

Curs acadèmic: 2011/2012 **Trimestre:** Tercer
Nom de l'assignatura: Estratègies de Seguretat en Xarxes i Serveis
Codi de l'assignatura: 21743
Estudis: Grau en Enginyeria Telemàtica, Grau en Enginyeria en Informàtica, Grau en Enginyeria de Sistemes Audiovisuals
Nombre de crèdits ECTS: 4 ECTS
Nombre total d'hores de dedicació: 100
Temporalització:
Curs: Tercer
Tipus: Trimestral
Període: Tercer Trimestre
Professorat: Vanesa Daza

Pla Docent

1. Dades descriptives de l'assignatura

- **Curs acadèmic:** 2011/2012
- **Nom de l'assignatura:** Estratègies de Seguretat en Xarxes i Serveis **Codi:** 21743
- **Tipus d'assignatura:** Optativa
- **Titulació / Estudis:** Grau en Enginyeria Telemàtica, Grau en Enginyeria en Informàtica, Grau en Enginyeria de Sistemes Audiovisuals
- **Nombre de crèdits ECTS:** 4
- **Nombre total d'hores de dedicació a l'assignatura:** 100 h
- **Temporalització:**
    - Curs: 3er curs
    - Tipus: trimestre
    - Període: 3er trimestre
- **Coordinació:** Vanesa Daza
- **Departament:** Departament de Tecnologies de la Informació i les Comunicacions
- **Professorat:** Vanesa Daza
- **Departament:** Departament de Tecnologies de la Informació i les Comunicacions
- **Llengua de docència:** Català
- **Edifici on s'imparteix l'assignatura:** Edifici 52 – Roc Boronat
- **Horari:**
  - Dilluns 10:30 – 12:30
  - Dimarts 12:30 – 14:30
  - Dimecres 8:30 – 10:30

2. Presentació de l'assignatura

Actualment no és difícil trobar al diari notícies que expliquen com les dades i els serveis de les empreses s'han vist compromeses per hackers. Inclús les principals companyies de tots els àmbits (webs, jocs en línia, e-banking, administració, ...), que operen principalment a través de la xarxa, s'han vist sotmeses a nombrosos atacs, com per exemple els atacs de denegació de servei (DoS), que aconsegueixen que caigui temporal o permanentment el servei.

Una forma per garantir la seguretat de la xarxa d'ordinadors d'una empresa és que s'abstinguin de posar-los connectats a Internet, i mantenint-los darrera d'una porta tancada amb clau, però encara hi ha atacs que poden realitzar els propis treballadors des de dintre (les estadístiques indiquen que d'un 70% o 80% es fan per personal de la pròpia empresa). Desafortunadament, però, aquesta no és una solució molt pràctica.

Avui dia, els equips són més útils si estan connectats en xarxa per compartir informació i recursos, però les empreses que posen els seus equips en xarxa necessiten prendre algunes precaucions senzilles per reduir les amenaces i el risc a que estaran sotmesos.

És crucial per a les organitzacions definir els objectius de seguretat per tal de poder establir els mecanismes i les metodologies que cal seguir per tal de poder-los aconseguir.

L'objectiu principal d'aquesta assignatura és treballar els principals aspectes implicats en el desplegament de mecanismes i procediments de gestió de la seguretat en les xarxes de telecomunicació, establint els principals principis de la seguretat de la informació, així com els principals atacs i contra-mesures coneguts. Així mateix es contemplaran aspectes tecnològics, regulatoris i d'avaluació de tecno-economia, tot descrivint les principals polítiques de seguretat, així com les principals metodologies d'anàlisis de riscos.

L'aproximació de l'assignatura és que, en algunes parts, l'alumne aprengui dels propis errors. Així, a partir d'algunes vulnerabilitats, els alumnes veuran la necessitat de garantir mecanismes de seguretat.

Tal i com es descriurà a l'apartat corresponent, l'assignatura inclou tant activitats pràctiques com estudi de casos.

3. Recomanacions

Es recomana que l'alumne hagi tingui els coneixements bàsics dels principals conceptes i protocols de xarxes, i que hauran assolit a l'assignatura *Xarxes i Serveis*.

4. Competències a assolir en l'assignatura

Competències generals	Competències específiques
Instrumentals 1. Habilitat de cerca i la gestió de la informació 2. Capacitat d'anàlisi i síntesi 3. Capacitat de comunicació oral 4. Capacitat de presa de decisions 5. Capacitat d'organització i planificació 6. Capacitat per aplicar els coneixements a l'anàlisi de situacions i la resolució de problemes **Interpersonals** 7. Capacitat crítica i autocrítica. 8. Compromís ètic. 9. Capacitat de treballar en un grup multidisciplinari i en un entorn multilingüe i de comunicar, tant per escrit com de forma oral, coneixements, procediments, resultats i idees relacionades amb les Tecnologies de la Informació **Sistèmiques** 10. Capacitat de resoldre problemes amb iniciativa, presa de decisions, creativitat, i de comunicar i transmetre coneixements, habilitats i destreses, comprenent la responsabilitat ètica i professional de l'activitat de l'enginyer TIC 11. Capacitat per progressar en els processos de formació i aprenentatge de manera autònoma i contínua 12. Capacitat de motivació per la qualitat i per l'assoliment 13. Capacitat de generació de noves idees	14. Capacitat per aplicar les tècniques en què es basen les xarxes, serveis i aplicacions telemàtiques per a garantir la seguretat (protocols criptogràfics, tunelatje, tallafocs, mecanismes de cobrament, d'autenticació i de protecció de continguts) 15. Identificar les amenaces més representatives per a la seguretat de la informació així com els atacs associats 16. Utilitzar bones pràctiques per garantir la seguretat física dels servidors i altres components de la xarxa 17. Conèixer la naturalesa dels virus informàtics, els mètodes de propagació, i els mitjans de protecció dels virus de les xarxes 18. Conèixer i utilitzar els principals protocols criptogràfics per garantir la seguretat a les comunicacions 19. Conèixer i utilitzar les eines pertinents per proporcionar seguretat de xarxa 20. Conèixer les principals metodologies de la gestió de riscos 21. Conèixer les principals lleis i regulacions relatives a la seguretat de la informació 22. Capacitat per a la redacció i desenvolupament de projectes en l'àmbit de la seva especialitat

5. Continguts

- Bloc 1. Principis de Seguretat de la Informació
- Bloc 2. Fonaments Criptogràfics
- Bloc 4. Aplicacions Malicioses
- Bloc 5. Seguretat de Xarxes
- Bloc 6. Seguretat Web
- Bloc 7. Seguretat Física
- Bloc 8. Polítiques de Seguretat
- Bloc 9. Anàlisi i Gestió de Riscos

6. Metodologia

Aquesta assignatura es durà a terme mitjançant sessions presencials i sessions no presencials.

Les sessions presencials seran tant sessions de teoria, com de seminaris i laboratoris. A continuació es detallen els trets bàsics de cada tipologia:

- **Sessions de Teoria:** Tindran una durada aproximada de dues hores. La professora presentarà durant aquestes sessions els conceptes, procediments i processos corresponents a cada un dels blocs temàtics. Tot i que tindran un caire fonamentalment expositiu hi ha interacció amb l'estudiant per a resoldre dubtes, plantejar qüestions, etc.

- **Sessions de Seminari:** Tindran una durada d'una hora. És important tenir present que **els seminaris requereixen d'un treball previ** que serà degudament comprovat mitjançant la realització d'un breu qüestionari a l'aula Global a l'inici de cada sessió de seminari. La no realització del qüestionari comporta l'anul·lació de qualsevol nota obtinguda com a resultat d'aquest seminari en concret.
  Durant la sessió de seminaris, a les quals es plantejaran un o diversos exercicis pràctics, els estudiants comptaran amb el suport del professor per a resoldre tots els dubtes que puguin sorgir.

- **Sessions de Laboratori:** Tindran una durada de dues hores. A les sessions de laboratori els alumnes participaran, al laboratori de xarxes, en l'anomenat "Simulated Secure Society"; un joc de rol. El treball serà grupal i la formació dels grups serà a partir de les fitxes d'habilitats que defineixen els diferents perfils/rols del joc.
  Els estudiants posaran en pràctica tots aquells coneixements i habilitats adquirits a les sessions de teoria i seminari, tot emulant un entorn pràctic.
  Mireu l'apartat *Simulated Secure Society* per a conèixer més detalls.

Serà a les **sessions no presencials** on:

- L'estudiantat prepararà les sessions de seminari tot consolidar els coneixements adquirits a les sessions de teoria de l'assignatura, contrastant amb fonts bibliogràfiques i enllaços facilitats pels professors.
- L'estudiantat prepararà la "partida" de joc de rol. Implicarà coordinació i reunions (virtuals o presencials) inter i entre grups.

Tot el material de l'assignatura (diapositives i enunciats) estarà disponible a l'Aula Global.

7. El Joc de Rol SimSecSoc (S^3)

A les sessions de laboratori de l'assignatura, s'implementarà el Joc de Rol *Simulated Security Society*. Com s'ha dit anteriorment, la distribució de rols/equips es realitzarà en funció del perfil formatiu/motivacional de cada estudiant.

ROLS:

- El **professor** responsable de les aules de laboratori serà el que exercirà de **màster** del joc i les seves tasques principals seran:
    - Descripció de l'escenari a simular
    - Descripció del joc durant el trimestre
    - Vetllar per al seguiment del joc de rol

- Els **estudiants** estaran dividits en dos grans grups (correspondrà al grup de laboratori al qual pertanyen) que representaran dues empreses fictícies amb una forta competència entre elles. Per exemple, dues empreses de rellotges: "Trolex S.A." i la "Trorion Corporation").
  Relacionats amb cada una de les empreses hi haurà 5 **Departaments**, concretament:
    - Departament de Comunicacions de l'empresa
    - Departament de Sistemes de l'empresa
    - Departament de Programació de l'empresa
    - L'agència de Certificació (empresa externa)
    - Banca on-line (empresa externa)

Cada Departament estarà format per 4 persones, a excepció del Departament de programació que constarà d'algun estudiant més. TOTS els Departaments segueixen una estructura interna idèntica, concretament, a cada Departament hi haurà els següents **rols/tasques**:

- Rol de Responsable: escollit de manera democràtica entre els diferents membres del grup. Funcions del Responsable: Dirigirà i es responsabilitzarà de les accions que hagin de realitzar el grup.
- Rol de Secretari: s'encarregarà de gestionar les reunions, (incloent la realització d'actes)
- Rol de Desenvolupador: liderarà els aspectes més tecnològics de les accions que s'hagin de prendre.

- Rol de Comercial: S'encarregarà de presentar la feina realitzada pel grup així com de les relacions que s'hagin d'establir amb la resta de grups).

OBJECTIU DEL JOC:

- Els respectius directors de Trolex i Trorion han vist les possibilitats que ofereix Internet, i han decidit recolzar les TIC. Esperen obrir una nova línia estratègica que demostri la modernitat dels seus respectius grups empresarials tot implementant una botiga on-line dels seus productes. D'altre banda cal tenir present que, en haver un alt grau de competitivitat entre ambdues empreses, la "lluita" per ser la millor estarà molt present, per tant, cap de les dues desaprofitarà cap moment per perjudicar la imatge de l'altre sent la botiga on-line el *camp de batalla*.
  La securització de tots els elements de la xarxa i de la pròpia botiga seran les claus per aconseguir l'èxit o el fracàs. La botiga es realitzarà de manera col·laborativa entre els diferents grups seguint les instruccions donades pel màster.
  L'objectiu doncs del joc és **alçar una empresa simulada i vetllar per la seva seguretat.**

ALTRES INFORMACIONS IMPORTANTS A TENIR EN COMPTE:

- Tot i que cada estudiant tindrà un rol concret dins del seu equip és important remarcar que **tots** els estudiants participaran en la implementació de l'acció o tasca per igual. Per tal d'ajustar el nombre de participants del grup amb la dificultat, en alguns departaments el rol de desenvolupador pot estar representat per més d'un estudiant sempre i quan la resta de rols hagin estat coberts.

- El joc de rol es presentarà el primer dia de classe, conjuntament a la resta de l'assignatura. Es sol·licitarà als alumnes que triïn el grup del qual volen formar part, via una consulta a l'aula Global de l'assignatura. Per a facilitar la tria a la presentació s'inclourà el llistat de tasques i habilitats que es treballaran en cadascun dels grups. Els grups tenen una mida limitada, i s'aniran tancant segons demanda dels alumnes. La consulta es **tancarà** a l'aula Global el dia **17 d'abril.** Aquells estudiants que no hagin participat a la consulta seran assignats en un grup pel professor responsable.

- Un cop establerts els grups, els alumnes disposaran d'una setmana per a assignar els seus rols dins del grup. El primer que es farà serà triar de manera democràtica al responsable del grup. Un cop triat, el responsable avaluarà quin és el millor rol per a la resta de companys del grup (considerant entrevistes, habilitats, preferències dels implicats,...). **Abans del 25 d'abril**, cada secretari de grup ha d'enviar al professorat responsable (màster) la composició dels rols del seu grup.

- Durant el joc, els alumnes tindran assignat un rol d'atacant ("hacker") que hauran de desenvolupar en certs moments de la pràctica. Es tractarà principalment d'intentar realitzar un atac concret requerit pel màster contra el

producte que s'estigui construint a la competència amb l'objectiu de malmetre la seva imatge o disminuir la seva eficiència . Els alumnes hauran de proposar en un informe un anàlisi de l'atac realitzar així com de les contramesures (si s'escauen) suggerides per a garantir la seguretat del producte final. Aquestes tasques es realitzaran a partir de la setmana 7 del curs.

- Es proposaran mesures per garantir la seguretat del producte final que hauran de ser implementades pels diferents grups.

- Finalment els alumnes disposaran del producte final de l'empresa de la competència per tal de que realitzar una anàlisi de seguretat, i en el cas de que sigui possible, realitzar algun atac (amb la proposta de contramesura). Aquests anàlisis en realitzaran segons els diferents departaments, que miraran d'analitzar els mecanismes i els procediments de la seva àrea.[1]L'última setmana del curs els alumnes disposaran del producte final en màquines virtuals. Els alumnes realitzaran un anàlisi exhaustiu per analitzar la seguretat i realitzar un informe sobre atacs i contramesures.

Nota: Tot plegat és un joc de rol simulat que no ha de sortir més enllà de l'entorn propi de l'assignatura amb la finalitat d'assolir els competències recollides.

8. Avaluació

Per a l'avaluació de l'assignatura es tindran en compte els següents elements:

- Qüestionaris on-line presencials (pre-seminaris)- (15%)
- Lliurament i presentació dels exercicis pràctics de seminari- (35%)
- Joc de rol (50%), que s'avaluarà segons els següents paràmetres:
  - Informe i presentació tasques realitzades del joc (inclou informe final de securització)- (25%)
  - Informe i presentació dels atacs realitzats així com de les solucions que es proposen per evitar l'atac- (20%)
  - Auto-avaluació del treball en equip- (15%)

A més a més, a les sessions de teoria es plantejarà una curt activitat a l'inici i al final de la sessió (p.e. mots encreuats, núvol de paraules,...). La participació activa en aquestes activitats (limitada a un llindar d'estudiants que primer realitzin l'activitat) pot representar fins a un 10% extra per a la puntuació final.

9. Bibliografia i recursos didàctics

La bibliografia i recursos didàctics de la primera part de l'assignatura són:

- Bibliografia bàsica

[1] Aquells departaments o estudiants a nivell individual que detectin algun altra forat de seguretat, poden realitzar (a més a més) un anàlisi que serà valorat sempre com a tasca positiva (en el cas de que efectivament es tracti d'un forat de seguretat) a tenir en compte en la valoració final. Seran especialmente valorats aquells que no hagin estat detectats per cap altre departament o estudiant.

  - Introduction to Computer Security, M. T. Goodrich, R. Tamassia. Ed. Pearson, 2011.
  - Principles of Information Security, 4th Edition, M. Whitman, H. Mattord, Cengage Ed., 2011.
- Bibliografia complementària
  - Cryptovirology, A. Young, M. Yung, Wiley, 2004.
- Recursos didàctics i material docent
  - A l'aula Global de l'assignatura, l'alumne podrà obtenir el material docent corresponent a les sessions de teoria.
  - A l'aula Global de l'assignatura, l'alumne podrà obtenir la col·lecció de problemes corresponent a les sessions de seminaris.

10. Planificació

	Dilluns 10.30-12.30	Dimarts 12.30-14.30	Dimecres 08.30-10.30
1 9 - 13 abr	FESTIU	T (B1)	T (B2)
2 16 - 20 abr	S101 S102	T (B3-1p)	S102 S101
3 23 - 27 abr	FESTIU	T (B3-2p)	S101 S102
4 30 abr-4 maig	NO CLASSE	FESTIU	L101
5 7 - 11 maig	L102	S102 S101	T (B4)
6 14 - 18 maig	S101 S102	T (B5)	S102 S101
7 21 - 25 maig	L101 Joc de Rol(1)	L102 Joc de Rol(1)	T (B6)
8 28 maig- 1 jun	FESTIU	S101 S102	T (B7)
9 4 - 8 jun	S102 S101	L102 Joc de Rol(2)	L101 Joc de Rol(2)
10 11 -15 jun	L101 Joc de Rol(3)	L102 Joc de Rol(3)	T (B8-B9)
11 18 -22 jun	L102 Joc de Rol(4)	L101 Joc de Rol(4)	Tutoria