ASIGNATURA DE MÁSTER:

SEGURIDAD EN REDES INDUSTRIALES

Curso 2016/2017

(Código:28803241)

1.PRESENTACIÓN

Las redes industriales son, por un lado, vitales y, por otro, vulnerables, con consecuencias potencialmente devastadoras en el caso de un incidente exitoso de ciberseguridad. Los ataques están evolucionando rápidamente, haciéndose más inteligentes y adaptables, difíciles de detectar y muy persistentes. Se habla ya de sabotajes industriales y de problemas en infraestructuras críticas. La tendencia es muy preocupante e implica la necesidad de profesionales mejor preparados, tanto desde el punto de vista puramente industrial como desde el punto de vista de la seguridad en redes y sistemas

Siguiendo este razonamiento, se puede expresar como objetivo general de esta asignatura el ubicar correctamente la seguridad informática como uno de los puntos clave a tener en cuenta en cualquier proceso de análisis, diseño, desarrollo y mantenimiento de sistemas de comunicación industrial, enseñando a valorar la importancia que debe tener y qué consecuencias, siempre negativas, podría tener el no hacerlo así.

2.CONTEXTUALIZACIÓN

Se trata de conseguir que los estudiantes obtengan el conocimiento de los principales problemas de seguridad informática relacionados con las redes industriales, tanto los de naturaleza física como los de naturaleza lógica. Asimismo se busca que los estudiantes obtengan el conocimiento de las principales soluciones técnicas y organizativas que se utilizan hoy en día en la industria para tratar de minimizar los riesgos asociados a tales problemas de seguridad. Este conocimiento debe además estar especialmente orientado a aspectos prácticos, por lo que se debe plantear al estudiante aspectos prácticos ligados a los conocimientos citados.

Es muy importante señalar desde el principio la necesidad previa de conocimientos de redes de comunicación, tanto industriales como (especialmente) de redes IP, así como unos conocimientos básicos de los ataques más habituales a la seguridad de sistemas y redes IP, y de las principales soluciones a estos problemas. Los alumnos que carezcan de estos requisitos previos DEBEN cursar previamente la asignatura “Aplicaciones Industriales de las comunicaciones” (código 28803256) del mismo itinerario de “Ingeniería Telemática” del Máster

3.REQUISITOS PREVIOS RECOMENDABLES

Es muy importante señalar desde el principio la necesidad previa de conocimientos de redes de comunicación, tanto industriales como (especialmente) de redes IP, así como unos conocimientos básicos de los ataques más habituales a la seguridad de sistemas y redes IP, y de las principales soluciones a estos problemas. Los alumnos que carezcan de estos requisitos previos DEBEN cursar previamente la asignatura “Aplicaciones Industriales de las comunicaciones” (código 28803256) del mismo itinerario de “Ingeniería Telemática” del Máster.

Además, es necesario tener un buen conocimiento de inglés técnico que le permita leer y comprender la parte de la bibliografía que está en ese idioma.

4.RESULTADOS DE APRENDIZAJE

Los resultados del aprendizaje que debe alcanzar el estudiante son:

- Identificar los diferentes tipos de ataques a redes, sistemas y datos en una organización, así como las soluciones más habituales empleadas para tratar de soslayarlos. Estudiar los diferentes protocolos de uso posible en las redes de comunicación estudiadas.
- Identificar las herramientas de seguridad más habituales como cortafuegos, sistemas de detección de intrusiones (IDS) o aplicaciones de análisis de vulnerabilidades. Entender para qué se deben aplicar y en qué casos.
- Entender, desde un punto de vista práctico, las diferentes aplicaciones de la criptografía a la seguridad informática, tanto en protocolos como en sistemas criptográficos, de manera que se comprenda cómo usar la firma digital o cómo se configura una red privada virtual.
- Identificar cuáles son los principales problemas de seguridad en redes industriales (DCS, SCADA, etc.)
- Ser capaz de asesorar sobre qué soluciones de seguridad dar a problemas concretos de seguridad en redes industriales
- Ser capaz de explicar las principales motivaciones de los ataques a redes industriales, así como las consecuencias de los mismos
- Ser capaz de hacer un análisis de riesgos en un sistema de comunicaciones industriales
- Identificar, y entender cómo funcionan, las soluciones más habituales a los problemas de seguridad en redes industriales: zonas, segmentaciones, conduits, etc.
- Ser capaz de aplicar una política de monitorización de la seguridad en redes industriales.

5.CONTENIDOS DE LA ASIGNATURA

Los contenidos temáticos principales son los siguientes:

1. Revisión de aspectos importantes generales de seguridad de redes IP

2. Revisión de herramientas de seguridad no criptográficas: cortafuegos, IDS, analizadores de vulnerabilidades

3. Revisión de criptografía aplicada: algoritmos, protocolos y sistemas criptográficos

4. Introducción a los problemas de seguridad en redes industriales: terminología, sistemas DCS y SCADA, protocolos y redes industriales

5. Diseño, arquitectura de red y protocolos en redes industriales

6. Principales problemas de seguridad en sistemas de control industrial: motivaciones, consecuencias, métodos de ataque

7. Evaluación de vulnerabilidades y riesgos en sistemas de control industrial

8. Introducción a las defensas básicas en redes industriales: zonas, *conduits*, segmentación de redes, anomalías y amenazas

9. Monitorización de la seguridad en redes industriales

6.EQUIPO DOCENTE

- GABRIEL DIAZ ORUETA
- SERGIO MARTIN GUTIERREZ
- ELIO SAN CRISTOBAL RUIZ

7.METODOLOGÍA

Conforme al espíritu del Espacio Europeo de Educación Superior (EEES), el trabajo en la asignatura y el proceso de evaluación es continuo a lo largo del curso y está de acuerdo con la carga de trabajo y organización del contenido dado en los apartados anteriores.

El estudio y preparación de los contenidos debe ser continuo desde el inicio del curso y, como se ha indicado, se debe seguir el orden dado a los temas. La orientación de la carga de trabajo que le debe suponer cada tema, que aparecerá en la Guía de Estudio en el curso virtual, le permitirá distribuir el estudio a lo largo del curso entre los meses de octubre y mayo.

El estudiante deberá realizar una serie de ejercicios que se propondrán durante el curso y participar en los debates que se propongan. Deberá realizar asimismo un trabajo final sobre una serie de temas que se propondrán en el curso virtual.

Esta asignatura NO tiene Prueba Presencial asociada, estando la evaluación completamente basada en los procedimientos comentados.

8.BIBLIOGRAFÍA BÁSICA

ISBN(13): 9780124201149
Título: INDUSTRIAL NETWORK SECURITY (Segunda)
Autor/es: Joel Thomas Langill ; Eric D. Knapp ;
Editorial: SYNGRESS

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

ISBN(13): 9788436267167
Título: PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES (2013)
Autor/es: Castro Gil, Manuel Alonso ; Ignacio Alzórriz ; San Cristóbal Ruiz, Elio ; Díaz Orueta, Gabriel ;
Editorial: UN.E.D.

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

Comentarios y anexos:

Para preparar y estudiar el contenido de cada uno de los temas, le indicamosla bibliografía que debe utilizar.

Esta bibliografía básica es la que usted debe conseguir y consultar para el estudio de cada tema, ya que es a partir de ella sobre la que hemos diseñado y desarrollado esta asignatura.

9.BIBLIOGRAFÍA COMPLEMENTARIA

Comentarios y anexos:

"*The Code Book, the Secret History of Codes and Code Breaking*", S. Singh, 2000, version interactiva disponible desde el curso virtual de la asignatura.

Es un gran clásico como introducción a la criptografía aplicada. Con un lenguaje sencillo y muchos ejemplos prácticos presenta al lector desde la historia de la criptografía hasta los últimos avances en criptografía cuántica. Desde hace ya varios años Singh permite distribuir, sólo con intenciones didácticas, la versión interactiva de la que se dispone en el curso virtual. Es importante señalar, no obstante, que este libro cubriría un curso entero de 8 meses sólo dedicado a criptografía.

Además el estudiante dispondrá de artículos y trabajos varios sobre los diferentes contenidos de seguridad en redes industriales, que intentaremos ir haciendo accesibles en el curso virtual de la asignatura.

10.RECURSOS DE APOYO AL ESTUDIO

Curso Virtual

La plataforma aLF de e-Learning de la UNED proporcionará el adecuado interfaz de interacción entre el alumno y sus profesores. aLF es una plataforma de e-Learning y colaboración que permite impartir y recibir formación, gestionar y compartir documentos, crear y participar en comunidades temáticas, así como realizar proyectos online. Se ofrecerán las herramientas necesarias para que, tanto el equipo docente como los estudiantes, encuentren la manera de compaginar tanto el trabajo individual como el aprendizaje cooperativo.

Videoconferencia

La videoconferencia se contempla como una posibilidad de comunicación bidireccional síncrona con los estudiantes, tal y como se recoge en el modelo metodológico de educación distancia propio de la UNED. La realización de videoconferencias se anunciara a los estudiantes con antelación suficiente en el curso virtual de la asignatura.

11.TUTORIZACIÓN Y SEGUIMIENTO

La tutorización de los alumnos se llevará a cabo a través de la plataforma de e-Learning aLF o directamente por correo electrónico con el equipo docente:

Gabriel Díaz Orueta - gdiaz@ieec.uned.es

Sergio Martín Gutiérrez - smartin@ieec.uned.es

Manuel Castro Gil - mcastro@ieec.uned.es

12.EVALUACIÓN DE LOS APRENDIZAJES

Esta asignatura NO tiene Prueba Presencial asociada

La nota de la asignatura se obtendrá fundamentalmente a partir de ejercicios, debates y trabajo final, que se realizan a lo largo del curso y que corresponden a la evaluación continua de conocimientos a distancia.

Los pesos de estos métodos de evaluación serán:

- un 35% de los ejercicios propuestos,

- un 15% por la participación en debates y, en general, en los foros y
- un 50% asociado a la nota del trabajo final.

En cualquier caso, para aprobar la asignatura el estudiante deberá realizar correctamente al menos un ejercicio, participar suficientemente en los debates y aprobar el trabajo final

13.COLABORADORES DOCENTES

Véase equipo docente.