SAMSUNG

Samsung **TECH INSTITUTE**

Curso UMA / Samsung

INTRODUCCIÓN A LA CIBERSEGURIDAD EN SISTEMAS INFORMÁTICOS

¡Desarrolla tu futuro!

www.uma.es/techinstitute

UNIVERSITAS MALACITANA

ANDALUCÍA TECH
Campus de Excelencia Internacional

ANDALUCÍA TECH

UNIVERSIDAD DE MÁLAGA

GUÍA DEL CURSO

INTRODUCCIÓN A LA CIBERSEGURIDAD EN SISTEMAS INFORMÁTICOS

Índice

Introducción a la Ciberseguridad en Sistemas Informáticos

Duración: 150 h
Fechas: 02/04/18 - 05/06/18
Semanas de aprendizaje: 10

1. Introducción

El curso "INTRODUCCIÓN A LA CIBERSEGURIDAD EN SISTEMAS INFORMÁTICOS" está destinado a alumnos o titulados de Formación Profesional con conocimientos informáticos relacionados con el contexto del curso. Éste se enmarca en el Programa Samsung-UMA Tech Institute, puesto en marcha a través del Vicerrectorado de Proyectos Estratégicos. Los cursos son financiados mediante este programa de Responsabilidad Social Corporativa de la empresa Samsung Electronics Iberia S.A.U. que apuesta por la empleabilidad de los jóvenes en el sector tecnológico. Por este motivo el curso es totalmente gratuito tanto para alumnos de la Universidad de Málaga como para jóvenes procedentes de estudios de Bachillerato y Formación Profesional.

El curso cuenta con cinco módulos formativos que pueden dividirse en tres bloques:

- El primer bloque está formado por el módulo 1 (30 horas). Se trata de un módulo dedicado a introducir al alumno en los fundamentos de la Ciberseguridad, comenzando con una exposición del tipo de amenazas a los sistemas informáticos. A continuación, se vinculan esas amenazas a los requisitos de seguridad y privacidad en redes y aplicaciones, y cómo se aborda desde esa perspectiva el diseño de mecanismos específicos.

- El segundo bloque consta de los módulos 2 y 3 (30+30 horas). El primero de los módulos se centra en la problemática de la seguridad en el área de los sistemas operativos, centrándose en los sistemas Windows y Linux. Esto sirve como base para abordar las soluciones de seguridad en aplicaciones y en paquetes como Office. El segundo de los módulos de este bloque focaliza su atención en las soluciones que intentan evitar los ataques en redes y, más concretament, en aquellas basadas en TCP/IP. Además, se analizan las implicaciones para la privacidad de los usuarios, tanto desde el punto de vista de los dispositivos de estos como de los escenarios más comunes en los que estos participan (entornos de redes sociales y en la nube).

- El tercer bloque también está formado por dos módulos, los módulos 4 y 5 (30+30 horas). El primero de los mismos estudia los distintos aspectos del hacking ético, incluyendo las herramientas disponibles, las técnicas para el descubrimiento de vulnerabilidades, y los procesos de escalada de privilegios. El segundo se centra en estudiar cómo revelar la actividad desplegada por el malware en un equipo y de qué manera pueden obtenerse evidencias que permitan proteger un equipo ante la ejecución de malware.

2. Profesores

López Muñoz, Francisco Javier

- Catedrático de Ingeniería Telemática de la UMA.
- Profesor en el Departamento de Lenguajes y Ciencias de la Computación.
- Director del Grupo de Investigación en Ciberseguridad "NICS Lab".

Alcaraz Tello, María Cristina

- Profesora Ayudante Doctor en el Área de Ingeniería Telemática.
- Doctora en Informática por la UMA.
- Licenciada en Informática por la UMA.

Navarrete Fernández, Gerardo

- Técnico del Centro de Investigación Ada Byron.
- Miembro del grupo de investigación NICS Lab.
- Licenciado en Informática por la UMA

Nieto Jiménez, Ana

- Investigadora de la UMA.
- Profesor Ayudante Doctor.

Onieva González, José Antonio

- Doctor en Informática por la UMA.
- Coautor del libro "Secure Multi-Party Non-Repudiation Protocols and Applications".

Román Castro, Rodrigo

- Especialista en seguridad de la información.

3. Resumen de contenidos por unidad formativa

La planificación del módulo formativo podrá verse modi cada por motivos imprevistos (rendimiento del grupo, disponibilidad de recursos, etc.) y por tanto no deberá considerarse como de nitiva y cerrada.

Módulo 1. Fundamentos de Ciberseguridad (30 horas)

- El objetivo de este módulo es servir de puente al alumno para situarse en el contexto de la ciberseguridad informática, aún sin tener conocimiento previo. Por este motivo se parte desde la historia de la seguridad informática, y se detallan conceptos fundamentales a alto nivel de requisito. El alumno adquiere durante este módulo la capacidad de entender la relevancia de la ciberseguridad en la informática actual y futura y, al finalizar el módulo, tendrá las nociones suficientes para poder aplicar algunos mecanismos básicos de protección ante amenazas y seguridad en las aplicaciones basadas en utilidades de cifrado.

Módulo 2. Seguridad en Sistemas Operativos (30 horas)

- Durante la realización de este módulo, el alumno adquirirá conocimientos básicos de seguridad en sistemas operativos, en particular para los sistemas Linux y Windows. El curso se iniciará abordando la historia de los sistemas operativos y cómo han evolucionado hacia sistemas con opciones de seguridad más complejas. Así mismo, se abordarán las aplicaciones de seguridad no nativas (no incluidas en el sistema operativo), como los antivirus. Durante el curso se realizarán prácticas guiadas sobre los sistemas más extendidos para identificar las propiedades de seguridad. Se abordará la seguridad en aplicaciones office debido a su gran difusión, y aspectos como la seguridad en periféricos, debido a que está siendo uno de los puntos de entrada a diversos problemas de seguridad en las organizaciones. Finalmente, también se abordará la necesidad de establecer un plan para iniciar y gestionar las copias de seguridad debidamente.

Módulo 3. Seguridad y Privacidad en Internet (30 horas)

- Este módulo tiene como objetivo mostrar al alumno cómo se transmite la información entre dispositivos, aplicaciones y servicios a través de Internet. A lo largo del temario se mostrarán cuáles son los principales mecanismos de comunicaciones, así como los protocolos empleados. A continuación, se expondrán las principales deficiencias y riesgos asociados al modelo de comunicaciones empleado en Internet. Se abordarán los mecanismos existentes para minimizar y/o solventar estos riesgos, a través de casos prácticos en Windows y Linux. La privacidad de los datos del usuario será un tema clave en la parte final del módulo. Aquí el alumno aprenderá a utilizar los dispositivos personales, y los servicios en la nube, teniendo presente los problemas de privacidad. Por otro lado, las redes sociales suponen otro grave problema de cara a la privacidad. Se harán sesiones prácticas qué permitan exponer los riesgos asociados a un mal uso de este tipo de servicios.

Módulo 4. Hacking Ético (30 horas)

- En este módulo el alumno adquirirá conocimientos sobre el hacking ético como herramienta para la identificación de vulnerabilidades y la prevención de amenazas. Durante el curso se hará hincapié en el uso de herramientas gratuitas para realizar esta labor. Fundamentalmente se emplearán distribuciones Linux de pen-testing (p.ej Kali Linux). Los ataques automáticos también se incluyen en este módulo con una doble vertiente. Por una parte, agilizar las tareas de análisis de vulnerabilidades, y por otra parte, poner de relevancia la facilidad para desplegar ataques de este tipo, en la que el atacante apenas emplea esfuerzo. El alumno aprenderá a emplear estas herramientas y a tomar conciencia de la responsabilidad en su utilización.

- Finalmente se aleccionará al alumno sobre cómo hacer uso de los repositorios web para la consulta de vulnerabilidades.

Módulo 5. Protección Ante Malware (30 horas)

- El módulo comienza con una parte teórica donde se explica al alumno el concepto "malware" y los tipos existentes. Cada tipo conlleva una serie de características específicas relativas al comportamiento, instalación en el equipo y mecanismos de propagación utilizados. El objetivo a continuación es mostrar al alumno cómo y dónde buscar estos rastros a nivel práctico. Se harán uso de máquinas virtualizadas donde desplegar malware real sobre sistemas Windows, con el fin de mostrar al alumno cómo rastrear evidencias generadas por su ejecución. Para ello se hará uso de un conjunto de herramientas de análisis, qué estarán disponibles para el usuario de manera que pueda emplearlas también en sus equipos personales. El objetivo final es tanto aprender cómo localizar estos rastros como determinar la mejor forma de eliminar la presencia de malware del sistema. Conociendo las técnicas de instalación y propagación, el alumno aprenderá a modificar su equipo para protegerlo. Además, se expondrán herramientas y métodos existentes orientados a paliar el alcance del malware en entornos Windows.

- Por último, se expondrá tanto a nivel teórico como práctico, como poder ejecutar malware de manera segura con el objetivo de observar las modificaciones que realiza en el sistema.

4. Objetivos

- Introducir a los alumnos en los fundamentos de ciberseguridad y a las amenazas principales a los sistemas informáticos.
- Enseñar a seleccionar mecanismos de seguridad en base a los requisitos de las aplicaciones.
- Presentar los problemas de seguridad en los sistemas operativos Windows y Linux.
- Presentar soluciones para evitar ataques en redes TCP/IP.
- Analizar las implicaciones de privacidad de los usuarios en Internet.
- Estudiar las herramientas de hacking ético y las técnicas para descubrir vulnerabilidades.
- Estudiar las herramientas que permiten obtener evidencias sobre la ejecución de malware en un equipo infectado.
- Conocer cómo defenderse frente a la presencia de malware en el equipo.

5. Metodología de impartición

El curso cuenta con cinco módulos formativos que pueden dividirse en tres bloques:

- El primer bloque está formado por el módulo 1 (30 horas). Se trata de un módulo dedicado a introducir al alumno en los fundamentos de la Ciberseguridad, comenzando con una exposición del tipo de amenazas a los sistemas informáticos. A continuación, se vinculan esas amenazas a los requisitos de seguridad y privacidad en redes y aplicaciones, y cómo se aborda desde esa perspectiva el diseño de mecanismos específicos.

- El segundo bloque consta de los módulos 2 y 3 (30+30 horas). El primero de los módulos se centra en la problemática de la seguridad en el área de los sistemas operativos, centrándose en los sistemas Windows y Linux. Esto sirve como base para abordar las soluciones de seguridad en aplicaciones y en paquetes como Office. El segundo de los módulos de este bloque focaliza su atención en las soluciones que intentan evitar los ataques en redes y, más concretament, en aquellas basadas en TCP/IP. Además, se analizan las implicaciones para la privacidad de los usuarios, tanto desde el punto de vista de los dispositivos de estos como de los escenarios más comunes en los que estos participan (entornos de redes sociales y en la nube).

- El tercer bloque también está formado por dos módulos, los módulos 4 y 5 (30+30 horas). El primero de los mismos estudia los distintos aspectos del hacking ético, incluyendo las herramientas disponibles, las técnicas para el descubrimiento de vulnerabilidades, y los procesos de escalada de privilegios. El segundo se centra en estudiar cómo revelar la actividad desplegada por el malware en un equipo y de qué manera pueden obtenerse evidencias que permitan proteger un equipo ante la ejecución de malware.

6. Evaluación

Dentro de cada módulo se definirán una serie de criterios para su evaluación correspondiente por parte del equipo docente. Así pues, en el **Módulo 1** se realizarán ejercicios de comprensión basados en pruebas tipo test y/o la realización de prácticas guiadas de laboratorio, adaptadas al contenido teórico del módulo. La evaluación calificativa del módulo consistirá en la valoración de dichas pruebas de concepto/trabajo de laboratorio continuado y en el examen final qué se realizará al completar el módulo. Las pruebas de evaluación cubrirán los criterios de competencias.

El **Módulo 2** comprende una parte teórica y su correspondiente práctica, qué demuestra que el alumno ha afianzado los conocimientos teóricos. El equipo docente calificará las competencias adquiridas por el alumno durante el curso basándose en el trabajo práctico realizado en el aula y la prueba final al completar el módulo.

La evaluación del **Módulo 3** consistirá en la realización de una prueba calificativa al final del módulo para evaluar la adquisición de capacidades de los alumnos, tanto de la parte teórica como del contenido práctico desarrollado en clase.

En el **Módulo 4** el alumno será evaluado atendiendo a los resultados obtenidos con el trabajo realizado en el aula, la participación activa y la superación de una prueba de conocimiento general que supone el 60% de la nota al final del módulo.

Finalmente, en el **Módulo 5** las capacidades del alumno serán evaluadas de acuerdo a un examen realizado al final del módulo. En él se abordarán tanto cuestiones relativas a la parte teórica como casos de infección y vías que el alumno debe realizar para determinar y erradicar la infección de malware.

7. Cronograma

El curso se impartirá del 2 de abril de 2018 al 5 de junio de 2018, de lunes a jueves en horario de 16:30-20:30.

L	M	X	J	
2	3	4	5	
9	10	11	12	ABRIL
16	17	18	19	
23	24	25	26	
30	1	2	3	
7	8	9	10	
14	15	16	17	MAYO
21	22	23	24	
28	29	30	31	
4	5			JUNIO

SAMSUNG

Samsung Tech Institute

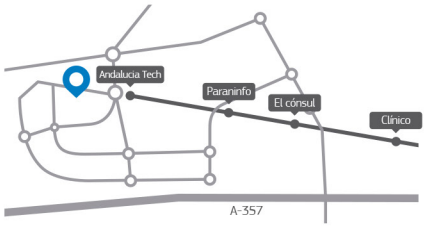
Ampliación del Campus de Teatinos

C/ Bulevar Luis Pasteur, 47

29071 Málaga

Más información en

www.uma.es/techinstitute



www.samsung.es

Síguenos en: