Guía Docente

DATOS DE IDENTIFICACIÓN

Titulación:	Diploma en Ciberseguridad y Hacking Ético (Título Propio asociado a Ingeniería Informática)
Rama de Conocimiento:	Ingeniería y Arquitectura
Facultad/Escuela:	Escuela Politécnica Superior
Asignatura:	Introducción a la Ciberseguridad
Tipo:	Propia Obligatoria
Créditos ECTS:	1,50
Curso:	1
Código:	56410
Periodo docente:	Primer semestre
Tipo de enseñanza:	Presencial
Idioma:	Castellano
Total de horas de dedicación del alumno:	37,50

Equipo Docente	Correo Electrónico
Francisco Martín Abreu	francisco.martin@ufv.es

DESCRIPCIÓN DE LA ASIGNATURA

El objetivo de esta asignatura es enseñar los conceptos básicos en torno a la Ciberseguridad en el mundo tanto Empresarial como de Consumo.

En concreto, los grandes bloques del curso serán:

1. Importancia de la Ciberseguridad en el mundo hiperconectado: (3hs)
2. Aspectos clave en la ciberseguridad empresarial (5h)
3. La ciberseguridad en el mundo de consumo (7h)

OBJETIVO

El objetivo final es que cada alumno tenga un conocimiento básico de las principales tendencias y elementos que configuran el mundo de la Ciberseguridad, tanto para la Empresa como el Consumidor final. De esta forma estará capacitado para abordar en más profundidad cada uno de los aspectos que componen la ciberseguridad

CONOCIMIENTOS PREVIOS

Fundamentos de Informática y Redes TCP/IP

CONTENIDOS

1. Introducción
1.1. Breve historia de la Ciberseguridad y ámbitos de la Ciberseguridad: Ciberataques contra las personas, contra las empresas, contra los gobiernos e IoT
1.2. Origen de los cibercriminales: Naciones, Terroristas, Espías industriales, Mafias de Crimen Organizado, Ciberdelincuentes en general, Trabajadores descontentos
2. Conceptos Básicos de Ciberseguridad
2.1. Ciberseguridad y Seguridad de la Información
2.2. Principios de la Seguridad de la Información
2.3. Etapas de un ciber-ataque
2.4. Clasificación de los ciber-ataques:
2.4.1. Según el sistema atacado: Computadores, Móviles, Redes, Infraestructuras, Personas
2.4.2. Según la relación del “target” con el atacante: “insider”, “outsider”
2.4.3. Según el impacto en el sistema atacado: activos, pasivos
2.4.4. Según el tipo de crimen: Ciber espionaje, Ciber terrorismo, Guerra cibernética, ciber asesinato, ciber crimen en general
2.4.5. Según el tipo de “Weaponization”: troyanos, macros, crackers, sql-injection, ataques xss, DDoS, backdoor, spoofing, snooping, man-in-yhe-middle
2.4.6. Según el mecanismo de “Delivery”: worm, spam, phishing, spear phishing, whale phishing, command and control, drive by, intrusion, zero-day exploit
2.4.7. Según el tipo de “Instalación”: aplicación, virus, rootkit, apt
2.4.8. Según la acción en el objetivo: spyware, keylogger, banker, adware, ransomware, credentials theft, crypto currency malware, bot, denegación de servicio, destrucción de datos, alteración de datos, toma de control del sistema, daño físico, muerte
3. “Best Practices”
3.1. ISO 27001
3.2. Prevención, Respuesta y Recuperación
3.3. Control de accesos a recursos
3.4. Política actualizaciones software
3.5. Business continuity and disaster recovery plan
3.6. Herramientas de seguridad preventivas
3.7. Security Event Monitoring
3.8. IoT Security
3.9. Auditorías de ciberseguridad
3.10. Penetration Testing y Vulnerability Assessment
3.11. Hacking ético
3.12. “Best Practices” por parte de los usuarios: uso de correo electrónico de la web y las aplicaciones. Gestión de datos
4. Técnicas usadas por las herramientas de ciberseguridad
4.1. Control de autenticación y accesos
4.2. Encriptado
4.3. Control de flujos de tráfico
4.4. BBDD reputación
4.5. BBDD firmas
4.6. BBDD botnets

4.7. BBDD de centros de comando y control
4.8. Listas blancas y negras
4.9. Análisis heurístico
4.10. Machine Learning
4.11. Sandboxing
4.12. Patrones de tráfico
5. Mecanismos de entrega de la ciberseguridad
5.1. “End-Point” Stand-alone
5.2. Gateway
5.3. Managed Security Service Provider (MSSP)(SOC)
5.4. SECurity as a Service (SECaSS)
5.5. Hybrid Mechanisms
5.6.Mobile Threat Defense (MTD)
5.7. Secure Access Service Edge (SASE)
6. Tipos de Herramientas de Ciberseguridad
6.1. End-Point Protection and Response (EPR): Anti-virus, Anti-Phishing, Anti-Spam, Anti-spayware, Anti-tracking, Ad-blocking (Anti-pop-ups), Filtrado de Contenido (Control Parental)
6.2. Firewall
6.3. Proxy
6.4. Secure Web Gateway
6.5. IDS/IPS 6.6.Data Leak Prevention (DLP)
6.7. UTM
6.8. Sandboxing
6.9. Anti-DDoS
6.10. MTD
6.11. IoT security tools
6.12. CASB
6.13. SASE
6.14. Firewall de aplicaciones
6.15. Encriptación (VPN, HTPS, encriptado almacenamiento…)
6.16. SIEM 7. Normativas y estándares
7.1. ISO 27001
7.2. GDPR
7.3. CIS 18
7.4. NIS 2

ACTIVIDADES FORMATIVAS

ACTIVIDAD PRESENCIAL
1. Lecciones expositivas donde se presentan y explican los distintos apartados de la asignatura, ilustrándolos con exposición de casos prácticos de actualidad o de especial relevancia
2. Presentaciones breves individuales por parte de los alumnos de casos reales de ciber-ataques actuales 3. Presentación de los trabajos en grupo
TRABAJO AUTÓNOMO/ACTIVIDAD NO PRESENCIAL
1. Trabajos en grupo. Estudio de un caso de ciber-ataque, analizando las distintas etápas del mismo. Elaboración de documento descriptivo del ciber-ataque y preparación de la presentación presencial
2. Preparación de la presentación presencial individual
3. Estudio de las materias presentadas en clase

DISTRIBUCIÓN DE LOS TIEMPOS DE TRABAJO

ACTIVIDAD PRESENCIAL	TRABAJO AUTÓNOMO/ACTIVIDAD NO PRESENCIAL
19 horas	18,50 horas

COMPETENCIAS

Conocer los origenes, historia y situación actual de la ciberseguridad

Conocimiento de los conceptos básicos de la ciberseguridad y la terminología específica de la materia

Conocimiento de los tipos principales de malware y ciberataques, de acuerdo a las etapas del ataque

Capacidad de análisis de un ciberataque, clasificándolo según las etapas del ataque y sabiendo como protegerse contra el mismo en las distintas etapas del ataque

Conocimiento de las principales herramientas de ciberseguridad disponibles, las técnicas utilizadas y los ciberataques de los que protege

Familiarización con los distintos mecanismos de entrega de la ciberseguridad

Capacitación para elaborar los componentes principales de un plan de Ciberseguridad

Conocimiento de las normativas generales existentes en lo referente a la ciberseguridad

RESULTADOS DE APRENDIZAJE

Entender a qué afecta y cómo afecta la seguridad hoy en día y a qué y cómo podría afectar en el futuro

Capacidad de entender cualquier proyecto relacionado con ciberseguridad

Capacidad de esbozar un plan de ciberseguridad de una organización

Capacidad de seleccionar las herramientas de ciberseguridad necesarias para un contexto determinado

Poder determinar la normativa y estándares apropiados para una situación determinada en relación a la ciberseguridad

SISTEMA DE EVALUACIÓN DEL APRENDIZAJE

La nota final del alumno tendrá en cuenta los siguientes factores:
[1] Prácticas / trabajos en grupo: Todas las prácticas son de entrega obligatoria. Cada una de ellas se evaluará de 0 a 10, no entregar una práctica supone recibir una calificación de 0 puntos en la misma. Para que una práctica se considere aprobada deberá obtener una calificación igual o superior a 5. El promedio de todas estas calificaciones prácticas reflejará el 40% de la calificación final. No realizar la práctica de acuerdo a la estructura especificada supondrá una calificación de 0 en esta prueba.
[2] Examen de carácter teórico que se realizará a la finalización del temario con el fin de evaluar la asimilación de conocimientos que ha realizado el alumnado de los contenidos de la asignatura. Se puntuará de 0 a 10 y reflejará Página 4 el 50% de la calificación final. Es necesario obtener en este examen una calificación mínima de 5 para superar la asignatura.
[3] Implicación y participación en clase. Esta nota reflejará, principalmente, la participación y actitud del alumno en las clases prácticas de la asignatura. Reflejará un 10% de la nota final. Respecto a este porcentaje será requisito imprescindible haber asistido como mínimo al 80% de las sesiones, en caso contrario este tipo de prueba se calificará con 0 puntos. Dentro de este 10% se evaluará también la calidad de las presentaciones en clase.
CÁLCULO DE LA NOTA FINAL: Teniendo en cuenta estos tres componentes, la nota final del alumno será un valor entre 0 y 10 y se calculará como: 0,4 * [1] + 0,5 * [2] + 0,1 * [3].

ALUMNOS CON DISPENSA ACADÉMICA O EN SEGUNDA MATRÍCULA O SUCESIVAS: Los alumnos que tengan concedida dispensa académica por causas justificadas o bien estén en segunda matrícula o sucesivas, estarán exentos de asistir a clase. Este hecho no exime de la obligación de realizar exámenes, prácticas y ejercicios en los mismos plazos que el resto de sus compañeros. Respecto del porcentaje del 10% correspondiente a participación en la asignatura y realización de ejercicios, será evaluado mediante la asistencia a un mínimo de una tutoría, en el horario convenido entre profesor y alumno. En dicha tutoría el alumno hará entrega de los ejercicios del curso y responderá a las preguntas que le efectúe el profesor sobre ellos.
RECUPERACIÓN EN CONVOCATORIA EXTRAORDINARIA: Los alumnos que no hayan alcanzado la nota mínima en el examen escrito o hayan suspendido en el computo de la nota global según la formula indicada más arriba, habiendo suspendido por tanto en la convocatoria ordinaria, podrán optar a una recuperación en la convocatoria extraordinaria, que consistirá en la evaluación de aquellas partes suspendidas en convocatoria ordinaria.
NORMATIVA ANTIPLAGIOS: Cualquier tipo de fraude o plagio por parte del alumno en una actividad evaluable, será sancionado según se recoge en la Normativa de Convivencia de la UFV. A estos efectos, se considerará "plagio" cualquier intento de defraudar el sistema de evaluación, como copia en ejercicios, exámenes, prácticas, trabajos o cualquier otro tipo de entrega, bien de otro compañero, bien de materiales o dispositivos no autorizados, con el fin de hacer creer al profesor que son propios.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

Francisco Martín Abreu Material disponible en el Aula Virtual de la asignatura.

Complementaria

J. David Irwin, Chwan-Hwa Wu Introduction to Computer Networks and Cybersecurity January 31, 2013