GUIA DOCENTE DEL CURSO
HACKING ÉTICO

AREA: DIGITAL BUSINESS
AUTOR: SPAIN BUSINESS SCHOOL

CÓDIGO: GD-730

IDENTIFICACIÓN DE LA ASIGNATURA

- Denominación: Hacking ético
- Código: 730
- Curso: 1
- Cuatrimestre: 1
- Carácter: Optativa
- Nº de créditos (horas): 15 ECTS (375 horas)
- Idioma en que se imparte: Español

REQUISITOS PREVIOS

No tiene requisitos previos, pero conocimientos básicos técnicos y de Linux sin recomendables.

PROFESORES Y CONFERENCIANTES

Juan Miguel González

- Categoría: Master
- Área funcional: Ciberseguridad
- Mail: juanmiguel.gonzalez@sbs.edu.es
- Tutorías: pedir cita previa

David Gaona

- Categoría: Máster
- Área funcional: Ciberseguridad
- Mail: david.gaona@sbs.edu.es
- Tutorías: pedir cita previa

DESCRIPCIÓN Y OBJETIVOS

Esta asignatura pretender dar unos conocimientos y capacidades de Hacking ético. Esto es una forma de referirse al acto de una persona, o mejor conocido como hacker, que utiliza sus conocimientos de informática y seguridad para encontrar vulnerabilidades o fallas de seguridad en el sistema, con el objetivo de reportarlas en la organización para que se tomen todas las medidas necesarias que posibilite prevenir una catástrofe cibernética, como el robo de información. Se estudiarán una serie de pruebas o test denominados "Test de penetración" cuyo objetivo es poder burlar las diferentes vallas de seguridad que tiene la red para diferentes organizaciones, con la única intención de probar su efectividad, o por el contrario, demostrar la vulnerabilidad de aquel sistema

Tiene por objetivos:

- Analizar algunas de las vulnerabilidades más importantes a nivel de sistema y de red.
- Ser capaz de realizar las distintas etapas de un test de penetración
- Conocer el funcionamiento de los cortafuegos y su uso en la seguridad de redes informáticas.
- Comprender los distintos tipos de sistemas de detección de intrusos y su aplicación en la seguridad informática.

COMPETENCIAS

Competencias generales

- Trabajar en equipos interdisciplinares (Competencias Interpersonales)
- Analizar sintetizar y organizar información masiva de grandes volúmenes de datos (Competencias Instrumentales)

Competencias específicas

- Adquirir las capacidades necesarias para obtener, mantener y procesar evidencias digitales utilizando procedimientos y herramientas específicas.
- Desarrollar técnicas y utilizar herramientas que exploten al máximo tus habilidades y conocimientos para la realización de pruebas de intrusión a sistemas y redes.
- Obtener una visión general e introductoria al mundo de la ciberseguridad, explicando los ataques más relevantes y cómo mitigarlos.
- Conocer el mundo de la ingeniería inversa y el análisis de código malicioso, asumiendo los procesos para entender el funcionamiento de los ficheros que trabajan a bajo nivel en sistemas y redes.
- Asimilar los conocimientos suficientes para gestionar y establecer unas políticas claras de seguridad para el componente móvil de un sistema de información.
- Conocer los fundamentos de la monitorización y correlación de eventos de seguridad, mediante el estudio, la elaboración e interpretación de informes reales.
- Realizar desarrollos en programación segura y mejorar tus habilidades en auditoría de seguridad en el análisis y evaluación del código fuente de las aplicaciones.
- Ser capaz de identificar, analizar y evaluar las vulnerabilidades y riesgos de seguridad de las redes, los sistemas informáticos y las aplicaciones.

- Ser capaz de diseñar y planificar estrategias de protección y defensa de entornos informáticos corporativos, basándose en las tecnologías y herramientas de seguridad informática existentes.

Conocimientos

- Ser capaces de asumir la responsabilidad de su propio desarrollo profesional y de su especialización en uno o más campos de estudio.
- Haber adquirido conocimientos avanzados y demostrado, en un contexto de investigación científica y tecnológica o altamente especializado, una comprensión detallada y fundamentada de los aspectos teóricos y prácticos y de la metodología de trabajo en uno o más campos de estudio.
- Saber aplicar e integrar sus conocimientos, la comprensión de estos, su fundamentación científica y sus capacidades de resolución de problemas en entornos nuevos y definidos de forma imprecisa, incluyendo contextos de carácter multidisciplinar tanto investigadores como profesionales altamente especializados.
- Ser capaces de predecir y controlar la evolución de situaciones complejas mediante el desarrollo de nuevas e innovadoras metodologías de trabajo adaptadas al ámbito científico/investigador, tecnológico o profesional concreto, en general multidisciplinar, en el que se desarrolle su actividad.
- Haber desarrollado la autonomía suficiente para participar en proyectos de investigación y colaboraciones científicas o tecnológicas dentro su ámbito temático, en contextos interdisciplinares y, en su caso, con una alta componente de transferencia del conocimiento

Destrezas

- Conoce los elementos vulnerables en el desarrollo de software y programa aplicaciones seguras.
- Demuestra que conoce y utiliza las Tecnologías de la Información y la Comunicación aplicadas a la Seguridad Informática.
- Conoce y aplica las herramientas para la búsqueda activa de empleo y el desarrollo de proyectos de emprendimiento.
- Demuestra habilidades para el trabajo cooperativo, la participación en equipos y la negociación, incorporando los valores de cooperación, esfuerzo, respecto y compromiso con la búsqueda de la calidad como signo de identidad.

TEMARIO / PROGRAMA ACADÉMICO

Recolección y escaneo de datos

- Recolección de Información y Anonimato
  - Introducción
  - Uso de herramientas de red (Whois, Traceroute, ping…)
  - Google dorks
  - Owasp-Mantra (http-headers, Passive-recon…)
  - Extracción de metadatos (FOCA)
  - Plugins de Firefox útiles
  - Técnicas OSINT
  - Ingeniería social
  - Uso de herramientas de Kali
  - Recolección de información de una red lan
  - Anonimato (Tor, uso de vpn)
- Escaneo
  - Análisis de servicios y puertos

        - Nmap (uso de la herramienta en sus distintos tipos de escaneo)
        - Evasión de firewalls
    - Análisis de vulnerabilidades
        - Clasificación de las mismas
        - Acunetix
        - Nessus
        - Cmsmap
        - Wpscan
        - Joomscan
        - Zap

Análisis y explotación

- Análisis de situación
- Búsqueda de exploits
- Ataque manual y automatizado
- Metasploit
- Ataque directo e inverso
- Pivoting
- Post-explotación
- Escala de privilegios
- Backdoors
- Extracción de información sensible y útil

Lenguajes de hacking

- Python
    - Introducción Python-hacking
    - Introducción a la programación Python
    - Uso de librerías específicas
- Ruby
    - Introducción Ruby-hacking
    - Introducción a la programación Ruby
    - Implementación a metasploit

Auditorías web

- Auditorías Web
- Taxonomía de un ataque
- Ejemplos de vulnerabilidades y ataques:
    - Inyección Sql
    - Xss
    - LFI
    - Inyección de código
    - RFI
    - Phising

Infraestructuras de hacking

- Hacking Infraestructuras
- Redes
    - Linux
    - Windows
    - OS
- Escalada de privilegios de cero a 100
    - Shell scripting
    - Linux
    - Windows

Auditoria de password y wifi

- Password Cracking
    - Diferencias entre tipos de ataque
    - Ataques on line y off line

    - Hashcat
    - Hydra
    - Ophcrack
    - Metasploit (auxiliares)
    - John
    - Cracking on line
- Auditoras WIFI
    - Uso de Airgeddon

Malware

- Malware
- Configuración de un troyano
- Uso de crypter
- Crypters on line
- Modding desde cero
- Evaluación del malware
- Métodos de infección

Informática forense

- Forense
- Introducción a la informática forense
- Evidencia digital
- Análisis de datos
- Mail
- Forense en redes y geo.
- Forense móviles
- Elaboración de informe

Realización informe pentest

RESULTADO DEL APRENDIZAJE

<<Los resultados de aprendizaje son declaraciones de lo que se espera que un estudiante conozca, comprenda y/o sea capaz de hacer al final de un proceso de formación y aprendizaje (ANECA 2022).
Se concretan en:

- *Conocimientos o contenidos que han sido comprendidos, mediante la asimilación de teorías, información, datos, etc.*
- *Habilidades o destrezas, actitudes y valores para aplicar conocimientos y utilizar técnicas a fin de completar tareas y resolver problemas.*
- *Capacidades demostradas para utilizar conocimientos, destrezas y habilidades personales, sociales y metodológicas en situaciones de trabajo o estudio y en el desarrollo profesional y personal. >>*

- Analizar las vulnerabilidades y saber evaluar los riesgos de las redes de computadores y sistemas informáticos.
- Manejar las técnicas y procedimientos actuales empleados en la evaluación de la seguridad.
- Integrar las tecnologías y herramientas de protección tanto de seguridad perimetral como de seguridad interna

ACTIVIDADES FORMATIVAS

<< Las actividades formativas que se realizarán en cada módulo/materia/asignatura (lo que corresponda). Para cada una de ellas se establecerá las horas de dedicación, porcentaje de presencialidad de dichas horas, y qué porcentaje de la actividad formativa implica interacción estudiantado/profesorado. Tal y como se indica en el Documento de REACU de 15 de enero de 2020 "Las actividades formativas desarrolladas a través de Internet, de modo sincrónico e interactivo, podrán equipararse a las actividades de tipo presencial de modo síncrono con las actividades formativas de tipo presencial.">>

En la asignatura se seguirán las actividades siguientes:

- Clases presenciales teóricas
- Prácticas con ordenador
- Seminarios
- Trabajos dirigidos
- Tutorías personalizadas
- Estudio y trabajo personal
- Pruebas presenciales (en directo) de evaluación

ACTIVIDADES PRESENCIALES	HORAS
Clases teóricas y prácticas en aula	75
Trabajos (trabajos con asesoramiento y presentación)	19
Tutorías presenciales (individuales o grupales) (5%)	26
Actividades de evaluación	10
	131 (35%)

Los alumnos de metodología virtual desarrollan las actividades presenciales en online síncrono.

METODOLOGÍA Y PLAN DE TRABAJO

La Universidad trabaja con 3 metodologías de enseñanza de clases en directo:

1) Presencial.
2) Semipresencial.
3) Online.

Además, cuenta con una cuarta metodología virtual o a distancia con clases asincronías y recursos de enseñanza (grabados), en la cual el alumno no asiste en directo a clases.

La definición de la presencialidad viene definida según se recoge en la guía de calidad universitaria descrita por ANECA (acreditadora oficial de la calidad universitaria en España) donde:

Presencial:

La metodología presencial se define como aquella que tiene presencia en directo del profesor docente, ya sea en aula o de manera virtual síncrona y siempre que supere un 34% de las horas correspondientes a los ECTS (1 ECTS son 25 horas de trabajo total).
En cada guía docente de la asignatura tendrá una definición concreta de la distribución de actividades presenciales y no presenciales, así como las horas de actividad formativa presencial por actividad concreta.

Definición en base a la guía de apoyo ANECA (Memoria de verificación de títulos 2023, ANECA Verifica). “Enseñanza presencial, aquella en la que la mayor parte de las actividades formativas se desarrollan preferentemente de forma presencial, es decir, interactuando el profesorado y el alumnado en el mismo espacio físico, sea éste el aula, laboratorios, espacios académicos especializados, etc. (presencia física y síncrona).” Y lo establecido en el RD 822/2021 en su artículo 14.7

Según definición de RD 1125/2003. Y define los siguientes tipos de actividades:

- Actividades presenciales. Son aquellas en las que el profesor o profesora está presente:

  - Actividades presenciales convencionales. Se refieren a las clases de teoría y/o problemas y a las prácticas de laboratorio o aula de informática. Suelen ser actividades sistemáticas y estar recogidas dentro del horario académico del centro.
  - Actividades presenciales no convencionales. El profesorado está presente, pero no están recogidas dentro del horario del centro: tutorías, pruebas de evaluación, seminarios, visitas, exposición de trabajos, etc.
- Actividades no presenciales. El profesor o profesora no está presente en ningún momento: estudio personal, preparación de trabajos e informes individuales o en grupo, etc.

Semipresencial:

SBS mezcla la metodología virtual con actividades síncronas y asíncronas. Las actividades síncronas obligatorias para el alumno son las pertenecientes a la evaluación de cada asignatura.

Definición en base a la guía de apoyo ANECA (Memoria de verificación de títulos 2023, ANECA Verifica). "Enseñanza semipresencial, aquella en que la gran mayoría de las actividades formativas previstas en el plan de estudios no requieren la presencia física del estudiantado y profesorado en el centro de impartición del título. Tal y como especifica el RD 822/2021 un título podrá definirse como semipresencial o híbrida si al menos el 40% -80% de los créditos que lo configuran se imparten en dicha modalidad."

Virtual:

SBS mezcla la metodología virtual con actividades síncronas y asíncronas. Las actividades síncronas obligatorias para el alumno son las pertenecientes a la evaluación de cada asignatura.

Definición en base a la guía de apoyo ANECA (Memoria de verificación de títulos 2023, ANECA Verifica). "Enseñanza virtual, aquella en que la gran mayoría de las actividades formativas previstas en el plan de estudios no requieren la presencia física del estudiantado y profesorado en el centro de impartición del título. Tal y como especifica el RD 822/2021 un título podrá definirse como virtual si al menos el 80% de los créditos que lo configuran se imparten en dicha modalidad."

Cabe destacar que la metodología de la Universidad es enriquecida dado que complementa los directos con recursos adicionales en el campus (cursos de la materia post-producidos, notas técnicas, casos prácticos, referencias adicionales, exámenes, etc.)

Sobre la definición anterior de las metodologías SBS, ¿cómo se trabajan a nivel educativo?

1) Presencial

   El alumno asiste presencialmente en aula entre 2-5 días por semana lo que confiere entre 8-20 horas de asistencia en aula semanales. El alumno debe complementar la enseñanza del aula con el estudio del campus virtual.
   Cada asignatura se configura en un número de ECTS. Cada ECTS son 25 horas totales y siguiendo la norma ANECA de estudios superiores, al menos el 34% de estas horas deben ser en acciones directas con el profesor (8,5). SBS, siguiendo la norma, realiza la siguiente distribución:
   - Al menos 5 horas de clase presencial en aula
   - 1-1,5 horas de evaluación (examen)
   - 1-1,5 horas de tutoría
   - 1-1,5 horas de trabajo práctico guiado por el profesor

   Cada asignatura cuenta con una guía docente donde queda definido particularmente el funcionamiento en el apartado de Actividades formativas.

2) Semipresencial

   El alumno asiste en directo entre 2-5 días por semana lo que confiere entre 8-20 horas de asistencia semanales (bien en presencial física en el aula u online directo

de la emisión). El alumno debe complementar la enseñanza del aula con el estudio del campus virtual.

Existe una variación a la metodología en la edición de febrero/marzo. El alumno asiste regularmente en aula los viernes sin limitación a que pudieran establecerse otros días presenciales en aula. Además, tiene entre semana días de clase online directo en una periodicidad entre 1 y 4 que complementa la acción presencial según recoge la guía. En esta variación el número de horas del alumno en directo (presencial aula o virtual) será de 6-14 h semanales.

3) Online

El alumno asiste de manera virtual a las clases, sin limitación a que pueda ser invitado por la escuela a algún periodo presencial en aula o bootcamp intensivo. Atendiendo a la definición del punto anterior, el alumno tendrá clases en directo de entre 8-20 horas semanales para la edición de septiembre/octubre y 6-14 horas para la edición de febrero/marzo.

Igualmente, el alumno debe complementar la enseñanza del aula con el estudio del campus virtual.

Es importante destacar que, con independencia de la metodología, los exámenes se realizan en directo, bien en aula o virtual con identificación y cámara para garantizar la veracidad del alumno. La parte práctica docente utiliza además de metodologías más tradicionales otras metodologías innovadoras basadas en:

- Aprendizaje basado en proyecto
- Estudios, análisis y exposiciones de métodos del caso
- Aprendizaje cooperativo y colaborativo
- Trabajo por ámbitos
- Gamificación educativa

SISTEMA DE EVALUACIÓN

La evaluación se llevará a cabo a través de las distintas pruebas de la asignatura:

- 100%. Examen final y pruebas prácticas de desarrollo sobre la materia.

Si hay casos prácticos se evalúan atendiendo a

1. Entrega de la memoria del caso
2. Exposición en público de este (en caso de ser un caso que requiera exponer, a decisión del profesor)

El examen tipo test es un examen de solución única en la que los fallos no restan. Se realiza en el campus online, en directo y siguiendo las instrucciones del profesor que puede ser presencial u online. Una vez se inicia el examen se genera uno específico para el alumno (distinto a otro pero de igual dificultad) que deberá realizarlo en ese momento. No puede salirse o dar para atrás en el navegador una vez visualizada la primera pregunta. Si sucediera alguna incidencia (corte de luz, internet, cierre inesperado, etc…) el examen se bloquea. Dicha incidencia debe ser reportada a la escuela quien analizar el comportamiento de uso anterior a la incidencia. Si es una incidencia se retomará un nuevo intento. Si hay algún indicio de fraude o engaño, el examen queda suspenso con la nota obtenida hasta el momento del corte o incidencia. No es alarmante, pero la escuela cuenta con un sistema antifraude.

Las fechas de examen, concretas a la edición, serán informados por el tutor principal de la asignatura.

BIBLIOGRAFÍAS

- Notas técnicas propias SBS
- Hacking Etico 101 : cómo hackear profesionalmente en 21 días o menos! : comprendiendo la mente del h. Edición: [2ª ed.] (actualizada a Kali 2.0). Autor: Astudillo, Karina B. Editorial: [United States] : CreateSpace, [2016] (C. Biblioteca)
- Seguridad informática : hacking Ético : conocer el ataque para una mejor defensa. Edición: 3ª ed. Autor: -. Editorial: Cornellá de Llobregat : ENI, 2015 (C. Biblioteca)
- Hacking web technologies. Edición: -. Autor: -. Editorial: Madrid : ZeroXword computing, 2016 (C. Biblioteca)
- SQL Injection. Edición: [3ª ed. rev. y amp.]. Autor: Rando González, Enrique. Editorial: Madrid : OxWord, 2016 (C. Biblioteca)
- Hacking y forensic : desarrolle sus propias herramientas en Python. Edición: -. Autor: Ebel, Franck. Editorial: Cornellá de Llobregat : Eni, 2016 (C. Biblioteca)
- Ethical hacking : teoría y práctica para la realización de un pentesting. Edición: -. Autor: González Pérez, Pablo. Editorial: Móstoles, Madrid : 0xWord, D.L. 2014 (C. Biblioteca)
- Hacking with Kali [Recurso electrónico] : practical penetration testing techniques. Edición: 1st ed. Autor: Broad, James. Editorial: Waltham, MA : Syngress, 2014 (C. Biblioteca)
- Ethical hacking : teoría y práctica para la realización de un pentesting . Edición: -. Autor: González Pérez, Pablo.. Editorial: 0xWord, (C. Biblioteca)