Información General del curso

Nombre del curso	ETHICAL HACKING
Código del curso	
Duración	20 horas

Descripción del curso

Este curso está orientado para aquellas personas que estén interesadas en comprender las técnicas y herramientas de hacking que se utilizan actualmente, así como también sacar provecho de las mismas para aumentar la seguridad de las organizaciones.

Como parte del curso el estudiante obtendrá el conocimiento necesario para identificar diferentes tipos de amenazas, ataques y vulnerabilidades en sistemas computacionales, para la aplicación de técnicas de hackeo que le permitan el desarrollo de habilidades técnicas en ciberseguridad. Al estudiante se le mostrará técnicamente cómo encontrar las debilidades y vulnerabilidades en los sistemas utilizando el mismo conocimiento y herramientas que un hacker profesional.

Este curso le presentará al estudiante ejemplos prácticos y dinámicos, con los que aprenderá cómo escanear, probar, explotar vulnerabilidades y asegurar sus propios sistemas. Los laboratorios darán a cada estudiante profundo conocimiento y experiencia práctica en: identificar amenazas cibernéticas, identificar vulnerabilidades en sistemas autónomos, generar vectores de ataque y explotar vulnerabilidades, con el fin de para presentar un informe de resultados con las debidas recomendaciones.

Lo anterior significa que los estudiantes, efectivamente deberán aprender a pensar y actuar como expertos en la disciplina del Ethical hacking, y no solo a comprender el marco conceptual de esta.

Objetivos generales y específicos

Objetivo general

Introducir al estudiante al mundo del Hacking Ético, dotándolo de conocimientos básicos para la identificación de diferentes tipos de amenazas, ataques y sobretodo

vulnerabilidades en sistemas computacionales, con el fin de que ponga en práctica dichos conocimientos técnicos de forma profesional.

Objetivos específicos

- Desarrollar habilidades técnicas de ataque y protección en el campo del Ethical Hacking.
- Identificar vulnerabilidades en sistemas autónomos.
- Analizar vectores de ataque para el aprovechamiento de vulnerabilidades.
- Presentar informes técnicos que describan las técnicas realizadas.

Contenidos

Temas
Módulo 1: Aplicación de la etapa de reconocimiento • Reconocimiento pasivo se consigue la información sin interacción directa con el objetivo mediante el uso de técnicas tales como la ingeniería social, sniffing de red, búsquedas por internet o vigilancia de instalaciones para recabar información sobre empleados, accesos, infraestructura, etc. • El reconocimiento activo comprende el estudio la red para descubrir los equipos individuales, las direcciones IP y los servicios que se prestan.
Módulo 2: Aplicación de la etapa de escaneo de información • En esta fase se usa la información proporcionada por el paso anterior para examinar la red. • Los hackers necesitan cualquier información que pueda ayudarles a llevar a cabo su ataque con éxito, alguna de la más común será: nombres de computadora, sistemas operativos, software utilizado, direcciones IP, cuentas de usuario, etc.
Módulo 3: Aplicación de la etapa de obtención de acceso • Se usa la información de las fases anteriores para explotar vulnerabilidades y acceder al sistema objetivo. • La explotación se puede realizar a través de una red de área local (LAN) – física o inalámbricamente -, por acceso local a un PC, por Internet, o de forma offline.
Módulo 4: Aplicación de la etapa de mantención de acceso y limpieza de rastros • Una vez realizada la intrusión en el sistema a través de la vulnerabilidad detectada, el objetivo del atacante o del hacker es mantenerse dentro del mismo.

- Se realiza nuevamente una comprobación para conseguir más información, identificar más vulnerabilidades, posibles redes para escalar privilegios y tener un total acceso.
- En esta fase se lleva a cabo la detección y eliminación de los rastros que demuestren la intrusión para no ser descubiertos y seguir teniendo acceso al objetivo sin levantar sospechas.

Metodología

El curso se desarrolla con una metodología virtual, donde los estudiantes analizan y desarrollan su aprendizaje a su propio ritmo, por medio de los videos y los recursos digitales disponibles, mientras que el 80% de su tiempo se dedica a realizar actividades prácticas, lo que los lleva a una comprensión más profunda de los contenidos, mediante una metodología de aprendizaje basada en proyectos ABP-STEM, la cual supone una manera concreta de aprender críticamente tomando elementos y problemas del contexto.

Esta experiencia de aprendizaje, constituye un modelo de instrucción auténtico en el que los estudiantes planean, implementan y evalúan proyectos que tienen aplicación en el mundo real más allá del aula de clase. En ella se recomiendan actividades interdisciplinarias, de largo plazo y centradas en el estudiante, en lugar de lecciones cortas y aisladas, más importante aún, los estudiantes encuentran los proyectos divertidos, motivadores y retadores, porque desempeñan en ellos un papel activo tanto en su escogencia como en todo el proceso de concepción, diseño, implementación y operación.

Estrategias de aprendizaje

El profesor escogerá los recursos que utilizará para la mediación pedagógica en el curso. Puede utilizar varios y/o todos los recursos que la plataforma Moodle tiene a su disposición, así como otros recursos que el profesor decida a conveniencia del curso. A continuación, se mencionan algunos:

- Cuestionarios: se utiliza para realizar evaluaciones iniciales, exámenes tipo test, pruebas de nivel

Evaluación

Exámenes cortos autoevaluados	Porcentaje
Examen corto 01 (fin de semana 01)	**25%**
Examen corto 02 (fin de semana 02)	**25%**
Examen corto 03 (fin de semana 03)	**25%**
Examen corto 04 (fin de semana 04)	**25%**
Total	**100%**

Recursos

Se cuenta con diversos medios tecnológicos para fomentar el aprendizaje según las estrategias de enseñanza que se puedan utilizar.

Se tienen plataformas virtuales propias (Campus Virtual de la Universidad) y de terceros (EBSCO, youtube, y facebook) para fomentar el aprendizaje según las estrategias de enseñanza. Las plataformas virtuales proveen de herramientas importantes como lo son foros, wikis, videos, portafolios y chats, para fomentar presentaciones y medios modernos de comunicación de la información. Particularmente en el curso se tiene acceso a:

- Campus Virtual de la Universidad
- EBSCO
- E-Libro
- Equipos colocados en la Nube con diferentes programas para la realización de ejercicios prácticos. Los mismos estarán debidamente seleccionados e identificados en el campus virtual de la Universidad Fidélitas en la sección de avisos generales.

Cada estudiante de Fidélitas tiene acceso a la licencia de Office 365 donde pueden descargar Office, Stream.

Bibliografía [EMC1]

Principal:

• Walker, M. (2019), CEH Certified Ethical Hacker Exam Guide, Fourth Edition. Mc Graw Hill Education

Bibliografía complementaria:

ElevenPaths, & Cebrián, J. M. A. (2016, 6 diciembre). ElevenPaths/FOCA. GitHub. https://github.com/ElevenPaths/FOCA

• DarkSec. (s. f.). DarkSecDevelopers/HiddenEye. GitHub. https://github.com/DarkSecDevelopers/HiddenEye

• Dewhurst, R. (s. f.). ethicalhack3r/DVWA. GitHub. https://github.com/ethicalhack3r/DVWA

• Bailey, M. (2011) Complete Guide to Internet Privacy, Anonymity & Security. (1ra Ed.) Nerel

• Bejitlich, R. (2013) The Practice of Network Security Monitoring: Understanding Incident Detection and Response. (1ra Ed.) noStarchPress

Cronograma

Semana	Contenidos	Actividades de Evaluación / Entregable
1	Aplicación de la etapa de reconocimiento	• Instalación y uso de sistema operativo víctima y atacante. • Configuración y uso de sniffer para controlar y analizar el tráfico red de un punto a otro de la misma. • Estudio de protocolos, puertos y servicios comunes.[EMC2]
2	Aplicación de la etapa de escaneo de información	• Escaneo de puertos con diferentes técnicas. • Uso de la técnica: Barrido de ping • Aprender a mapear una red • Uso de escáneres de vulnerabilidades
3	Aplicación de la etapa de obtención de acceso	• Identificar exploits comunes con la herramienta Searchexploit. • Aprender cómo se hace un ataque man in the middle. • Aprender cómo se hace un ataque DoS (denial of service). • Aprender técnicas para obtención de contraseñas
4	Aplicación de la etapa de mantención de acceso y limpieza de rastros	• Uso de y configuración de: • Aprender cómo se configura un Backdoor. • Aprender cómo se configura un Troyano. • Aprender cómo se hace una escalación de privilegios. • Aprender el uso de Rootkits.

MasterClass	**Fecha y hora** **14 de octubre 5 a 8**	**Modalidad: virtual remota a través de Teams**

Horas de oficina (Atención a estudiantes de manera remota vía Teams)	**Horario** **Miércoles de 5 a 5:30 pm**