DATOS GENERALES DEL CURSO

Escuela	Ciberseguridad
Código del curso	ACTI-HACK-1
Nombre del Curso	Certified Ethical Hacker EC Council
Horas totales de lecciones	40
Semanas totales del curso	10
Horas por sesión	4 (a la semana)
Horas extraclase	6 (a la semana)

DESCRIPCIÓN DEL CURSO

El curso se enfoca en el aprendizaje de los conceptos básicos de Hacker Ético a través de una metodología de EC-Council, que incluye actividades prácticas como parte esencial del aprendizaje, la cual le plantea al estudiante diferentes retos que debe solucionar a lo largo del programa, al final presentar un trabajo escrito y optar por examen para ganar certificación correspondiente dada por EC-Council.

REQUISITOS PREVIOS O DE INGRESO

- El estudiante debe contar con conocimiento básico a nivel técnico de Sistemas Operativos, Telecomunicaciones, y conocimiento del idioma inglés escrito.

Este curso está dirigido a:

- Profesionales en Seguridad de la Información
- Encargados de Unidades de Respuesta a Incidentes
- Profesionales de Tics
- Personal de SOCs
- Personal de C-SIRT
- Personal de Auditorias de seguridad informática
- Pentester

OBJETIVO GENERAL

Adquirir un conocimiento para entender los componentes de Hacker Ético en donde requiera aplicarlo.

OBJETIVOS ESPECÍFICOS

- Dominar el uso de la jerga básica para la comunicación en trabajos de Hacker Ético.
- Conocer las herramientas y métodos de los Hacker Ético
- Comprender la importancia de la ética y correcta función de la tarea de un de Hacker Ético
- Ser capaz de implementar un equipo de Hacker Ético en su ambiente seguro.

CONTENIDO

1. Introduction to Ethical Hacking

   Footprinting and Reconnaissance

2. Scanning Networks

   Enumeration

3. Vulnerability Analysis

   System Hacking

4. Malware Threats

   Sniffing

5. Social Engineering

   Denial-of-Service

6. Session Hijacking

   Evading IDS, Firewalls, and Honeypots

7. Hacking Web Servers

   Hacking Web Applications

8. SQL Injection

   Hacking Wireless Networks

9. Hacking Mobile Platforms

   IoT Hacking

10. Cloud Computing

    Cryptography

METODOLOGÍA

En el curso se usará la metodología 40-40-20 en la que se distribuye el tiempo de desarrollo de la clase en un 40% para presentación de contenidos, conceptos, modelos, ejemplos, de forma magistral por parte del docente. Luego un 40% del tiempo se dedica a realizar práctica acerca de los conceptos vistos en clase, por medio de talleres, laboratorios, prácticas guiadas, ejercicios, estudio de casos, laboratorios, entre otros. Y finalmente un 20% del final de la clase se utiliza para revisar la solución a la práctica

realizada, ofreciendo retroalimentación a los estudiantes, resolviendo dudas y haciendo el cierre de la clase.

Para seguir la metodología 40-40-20, se combinarán diversas actividades:

- Exposición de los conceptos con técnicas avanzadas de Hacker Ético para investigación de vulnerabilidades y explotarlas
- Prácticas guiadas donde los estudiantes podrán acceder, conocer y entender el funcionamiento de las herramientas utilizadas para la práctica de Hacker Ético
- Tareas prácticas en donde los estudiantes integran conocimientos para resolver problemas con ilabs y materia oficial para el curso.

ESTRATEGIAS DE APRENDIZAJE

Las estrategias de aprendizaje que el estudiante debe adoptar para lograr cumplir los objetivos del curso son:

- **Prácticas en clase**: Ejercicios prácticos que se realizan en clase de manera individual, en donde los estudiantes deben aplicar el conocimiento aprendido.
- **Laboratorios en clase**: Son laboratorios desarrollados por los estudiantes en computadora y bajo la guía y supervisión del profesor respetando las guías facilitadas por EC-Council
- **Lecturas extraclase**: Las lecturas extraclase se hacen con el material proporcionado por EC-Council. Todas las lecturas son en inglés.
- **Trabajo escrito**: El estudiante preparara un tema que el profesor considere pertinente, el cual les ayudará a reforzar lo visto en clase, cada trabajo incorporará un elemento práctico en el cual demuestren las habilidades adquiridas.

RECURSOS DIDÁCTICOS

- Se utilizará para todas las sesiones del curso presentaciones en proyector digital, que contendrán los conceptos correspondientes a cada sesión.
- Se utilizará un laboratorio de computadoras, con el software necesario para el desarrollo de los ejercicios.
- Se tendrá acceso en línea a la plataforma ilabs para realizar los ejercicios.

EVALUACIÓN

A continuación, se especifica la evaluación del curso, teniendo en cuenta su función sumativa, diagnóstica y formativa:

Concepto	Ponderación
Prácticas en clase (8 prácticas de 7,5% cada una)	60%
Asistencia	20%
Trabajo escrito	20%
Total	**100%**

Las prácticas en clase se realizan de manera semanal y serán individuales grupales. Durante cada laboratorio se aclaran las dudas que los estudiantes puedan tener y después de cada laboratorio el profesor, en conjunto con los estudiantes, verifica la solución correcta al problema planteado. Todos los laboratorios se entregan al profesor y son calificados.

El curso se aprueba con una nota ponderada mayor o igual a 70 (>=70) y una asistencia >=85%; de lo contrario el estudiante pierde el curso.

CRONOGRAMA

Semana	Sesión	Contenidos y actividades
1	1	**Presentación de contenidos:** Introduction to Ethical Hacking (40 minutos) **Pausa activa:** 5 minutos **Presentación de contenidos:** Footprinting and Reconnaissance (40 minutos) **Pausa activa:** 15 minutos **Actividad en clase**: Práctica en clase 1 (80 minutos) **Retroalimentación:** revisión de solución de la actividad en clase, resolución de dudas, discusión, análisis y cierre de la clase. (40 minutos) **Actividad extraclase**: Se trabaja en los pendientes de la práctica 1. (Tiempo estimado: 6 horas)
2	2	**Presentación de contenidos:** Scanning Networks (40 minutos) **Pausa activa:** 5 minutos **Presentación de contenidos:** Enumeration (40 minutos) **Pausa activa:** 15 minutos **Actividad en clase**: Práctica en clase 2 (80 minutos) **Retroalimentación:** revisión de solución de la actividad en clase, resolución de dudas, discusión, análisis y cierre de la clase. (40 minutos) **Actividad extraclase**: Se trabaja en los pendientes de la práctica 2. (Tiempo estimado: 6 horas)
3	3	**Presentación de contenidos:** Vulnerability Analysis (40 minutos) **Pausa activa:** 5 minutos **Presentación de contenidos:** System Hacking (40 minutos)

		Pausa activa: 15 minutos **Actividad en clase**: Práctica en clase 3 (80 minutos) **Retroalimentación:** revisión de solución de la actividad en clase, resolución de dudas, discusión, análisis y cierre de la clase. (40 minutos) **Actividad extraclase**: Se trabaja en los pendientes de la práctica 3. (Tiempo estimado: 6 horas)
4	4	**Presentación de contenidos:** Malware Threats (40 minutos) **Pausa activa:** 5 minutos **Presentación de contenidos:** Sniffing (40 minutos) **Pausa activa:** 15 minutos **Actividad en clase**: Práctica en clase 4 (80 minutos) **Retroalimentación:** revisión de solución de la actividad en clase, resolución de dudas, discusión, análisis y cierre de la clase. (40 minutos) **Actividad extraclase**: Se trabaja en los pendientes de la práctica 4. (Tiempo estimado: 6 horas)
5	5	**Presentación de contenidos:** Social Engineering (40 minutos) **Pausa activa:** 5 minutos **Presentación de contenidos:** Denial-of-Service (40 minutos) **Pausa activa:** 15 minutos **Actividad en clase**: Práctica en clase 5 (80 minutos) **Retroalimentación:** revisión de solución de la actividad en clase, resolución de dudas, discusión, análisis y cierre de la clase. (40 minutos) **Actividad extraclase**: Se trabaja en los pendientes de la práctica 5 (Tiempo estimado: 6 horas)
6	6	**Presentación de contenidos:** Session Hijacking (40 minutos) **Pausa activa:** 5 minutos **Presentación de contenidos:** Evading IDS, Firewalls, and Honeypots (40 minutos) **Pausa activa:** 15 minutos **Actividad en clase**: Práctica en clase 6 (80 minutos) **Retroalimentación:** revisión de solución de la actividad en clase, resolución de dudas, discusión, análisis y cierre de la clase. (40 minutos)

		Actividad extraclase: Se trabaja en los pendientes de la práctica 6. (Tiempo estimado: 6 horas)
7	7	**Presentación de contenidos:** Hacking Web Servers (40 minutos) **Pausa activa:** 5 minutos **Presentación de contenidos:** Hacking Web Applications (40 minutos) **Pausa activa:** 15 minutos **Actividad en clase**: Práctica en clase 7 (80 minutos). **Retroalimentación:** revisión de solución de la actividad en clase, resolución de dudas, discusión, análisis y cierre de la clase. (40 minutos) **Actividad extraclase**: Se trabaja en los pendientes de la práctica 7. (Tiempo estimado: 6 horas)
8	8	**Presentación de contenidos:** SQL Injection (40 minutos) **Pausa activa:** 5 minutos **Presentación de contenidos:** Hacking Wireless Networks (40 minutos) **Pausa activa:** 15 minutos **Actividad en clase**: Práctica en clase 8 (80 minutos) **Retroalimentación:** revisión de solución de la actividad en clase, resolución de dudas, discusión, análisis y cierre de la clase. (40 minutos) **Actividad extraclase**: Se trabaja en los pendientes de la práctica 8. (Tiempo estimado: 6 horas)
9	9	**Presentación de contenidos:** Hacking Mobile Platforms (40 minutos) **Pausa activa:** 5 minutos **Presentación de contenidos:** IoT Hacking (40 minutos) **Pausa activa:** 15 minutos **Actividad en clase**: Trabajo en clase dedicado al trabajo escrito. Se realizan prácticas recomendadas por EC-Council pero no calificadas (80 minutos) **Retroalimentación:** revisión de solución de la actividad en clase, resolución de dudas, discusión, análisis y cierre de la clase. (40 minutos) **Actividad extraclase**: Se trabaja en los pendientes del trabajo escrito. (Tiempo estimado: 6 horas)

10	10	**Presentación de contenidos:** Cloud Computing. (40 minutos) **Pausa activa:** 5 minutos **Presentación de contenidos:** Cryptography. (40 minutos) **Pausa activa:** 15 minutos **Actividad en clase**: Trabajo en clase dedicado al trabajo escrito. Se realizan prácticas recomendadas por EC-Council pero no calificadas (80 minutos) **Retroalimentación:** revisión de la solución del trabajo escrito, resolución de dudas, discusión, análisis y cierre de la clase. (20 minutos)
11	-	**Semana de entrega de notas, cierre del curso y trámite de insignias digitales.**