1.- Identificación de la Unidad de Aprendizaje					
Nombre de la Unidad de Aprendizaje					
HACKEO ETICO (CIBERSEGURIDAD)					
Clave de la UA	**Modalidad de la UA**	**Tipo de UA**		**Valor de créditos**	**Área de formación**
IH091	*Presencial*	*Curso -Taller*		6	Es
Hora semana		**Horas teoría/semestre**	**Horas práctica/ semestre**	**Total de horas:**	**Seriación**
3		40	20	60	N/A
Departamento			**Academia**		
Cs. de la Información y Desarrollos Tecnológicos			*Software de Sistemas*		

Presentación

Ciberseguridad además de prevenir y detectar riesgos y amenazas hacia un sistema informático, incluye estrategias tecnológicas ofensivas como contra-ataque a los adversarios; resguardar la privacidad e integridad de los datos e información ante ataques maliciosos es tema de suma importancia en la industria y gobierno.
El alumno debe conocer los temas de ciberseguridad como parte de las necesidades de su vida diaria y como un requisito de conocimiento en la administración y desarrollo de sistemas de información para la industria.

Tipos de saberes

Saber (Conocimientos)	Saber hacer (Habilidades)	Saber ser (Actitudes y valores)
Elementos esenciales del funcionamiento de los sistemas operativos Conocimientos básicos de administración de ambientes Linux y Windows Elementos esenciales en el funcionamiento de redes de cómputo. Conocimientos fundamentales de protocolos de red	Aplica los conocimientos teóricos en la práctica. Organiza y planifica. Analiza información, deduce procesos. Analiza y resuelve problemas. Creativo e innovador en el proceso de diseño y desarrollo de sistemas.	Compromiso con su formación personal y en su caso con el equipo de trabajo. Interés por aprender y trabajar. Responsabilidad. Respeto. Tolerancia. Honestidad. Ética Profesional. Liderazgo.

Competencia genérica	**Competencia profesional**

Realiza trabajo de manera individual y en equipo, con liderazgo aplicando las Ciencias Computacionales en la solución de problemas de su entorno. Aplica herramientas de programación y principios de Ingeniería de software para eficiente los procesos.	Identifica riesgos potenciales en el ciber-entorno; diseña estrategias a fin de proponer alternativas para gestionarlo adecuadamente.

Saberes previos del alumno

El alumno deberá contar con conocimientos de: lógica, protocolos de red, funciones del sistema operativo, funciones de software (middleware) y aplicaciones, abstraer y sintetizar problemáticas, trabajo colaborativo.

Perfil de egreso al que se abona

Capacidad de investigar, comprender, modelar y proponer soluciones a problemas de alta complejidad que se identifiquen en organizaciones de diversos tipos y entornos.

Perfil deseable del docente

Formación profesional.

El docente deberá contar preferentemente con un posgrado y/o al menos con una licenciatura afín al área de cómputo, deberá tener amplia experiencia en seguridad informática, preferentemente alguna certificación como CEH, CISSP, etc., que asegure su actualización periódica

Habilidades.

-Usar y manejar ambientes virtuales para el proceso de enseñanza aprendizaje.
Utilizar las TIC para diversificar y fortalecer las estrategias de aprendizaje por competencia.
-Fomentar actividades grupales que propicien la comunicación, el intercambio argumentado de ideas, la reflexión, la integración y la colaboración de y entre los estudiantes.
-Relacionar los contenidos de esta asignatura con las demás del plan de estudios a las que ésta da soporte para desarrollar una visión interdisciplinaria en el estudiante.
-Mostrar flexibilidad en el seguimiento del proceso formativo y propiciar la interacción entre los estudiantes.
-Tomar en cuenta el conocimiento de los estudiantes como punto de partida y como obstáculo para la construcción de nuevos conocimientos.
-Autorregular los procesos de aprendizaje.
-Propiciar actividades de búsqueda, selección y análisis de información en distintas fuentes.

2.- Contenidos temáticos

Contenido

1. **Introducción al hackeo ético**

1.1 Que es un hacker ético?
1.2 Vulnerabilidad, Exploit, Threat Agent, Threat
1.3 Riesgo

1.4 Gobernanza
- Políticas
- Estándares
- Procedimientos

1.5 CIA – Confidencialidad, Integridad, Disponibilidad
1.6 Metodologías de Hacking
- OSSTMM (Open-Source Security Testing Methodology Manual).
- ISSAF (Information Systems Security Assessment Framework).
- OWASP (Open Web Application Security Project).
- CEH (Certified Ethical Hacker).
- OS (OFFENSIVE SECURITY).

2. Fundamentos de Sistemas

2.1 Básico de Redes
- Modelo OSI
- Topologías de Red

2.2 Suite TCP/IP
- Direccionamiento
  - Físico
  - Lógico
- Protocolo TCP y UDP
- Puertos

2.3 Básicos de Sistemas operativos
2.4 Tecnología de Seguridad
- Firewalls
- IDS, IPS
- SIEM

3. Obtención de Información (reconocimiento) y Escaneo

3.1 Reconocimiento Pasivo
- Herramientas

3.2 Reconocimiento Activo
- Herramientas

3.3 Tipos de escaneo
- Herramientas

3.4 Enumeración
- Definición de la ruta de ataque

4. Hackeo Ético e ingeniería social

4.1 Método de búsqueda de exploits conocidos
4.2 Tipos de ataques
- Denial of Service (DoS)
- Distributed Denia lof Service (DDos)
- Web Application Attack
  - Command Injection

- SQL Injection
- Cross Site Scripting (XSS)

4.3 Autenticación
- Herramientas

4.4 Que es ingeniería social?
4.5 Tipos de ingeniería social?
- Física
- Phishing
- Web Sites

Estrategias generales para impartir la unidad de aprendizaje

1.Aprendizaje basado en resolución de problemas 2. Aprendizaje basado en casos de estudio 3. Prácticas guiadas. 4.Aprendizaje basado en proyectos 5. Solución de problemas de un contexto específico. 6. Mapas Mentales. 7.Textos argumentativos. 8. Participación en foros y debates.

Módulo I

INTRODUCCION AL HACKEO ETICO

Competencia Específica

Conocer los conceptos básicos relacionados al Hackeo, que le permitan identificar las metodologías de ataque y riesgos potenciales en el contexto cibernético.

Tipos de saberes

Saber (Conocimientos)	Saber hacer (Habilidades)	Saber ser (Actitudes y valores)
Hacker vs. Cracker. Conceptos teórico-básicos de la ciberseguridad. Tipos de ataques y atacantes. Políticas, estándares y procedimientos en gobernanza. Triangulo de la ciber-seguridad. Metodologías de hacking.	Aplica los conocimientos teóricos en la práctica. Organiza y planifica. Analiza información, deduce de procesos. Analiza y resuelve problemas. Creativo e innovador en el proceso de diseño y desarrollo de sistemas.	Compromiso con su formación personal y en su caso con el equipo de trabajo. Interés por aprender y trabajar. Responsabilidad. Respeto. Tolerancia. Honestidad. Ética Profesional.

Módulo II

FUNDAMENTOS DE SISTEMAS

Competencia Específica

Relacionar los conceptos y mecanismos de interacción en la comunicación en red entre sistemas operativos para formular estrategias de seguimiento y solución a problemas de seguridad.

Tipos de saberes		
Saber (Conocimientos)	Saber hacer (Habilidades)	Saber ser (Actitudes y valores)
Elementos esenciales del funcionamiento de los sistemas operativos Conocimientos básicos de administración de ambientes Linux y Windows Elementos esenciales en el funcionamiento de redes de cómputo. Conocimientos fundamentales de protocolos de red	Aplica los conocimientos teóricos en la práctica. Organiza y planifica. Analiza información, deduce procesos.	Compromiso con su formación personal y en su caso con el equipo de trabajo. Interés por aprender y trabajar. Liderazgo. Ética Profesional.
Módulo III		
OBTENCION DE INFORMACION (RECONOCIMIENTO) Y ESCANEO		
Competencia Específica		
Identificar en el proceso de ciber-ataque las estrategias de obtención de información y escaneo de sistemas que permitan al estudiante formular políticas de seguridad en la administración de sistemas.		
Tipos de saberes		
Saber (Conocimientos)	Saber hacer (Habilidades)	Saber ser (Actitudes y valores)
Tipos de reconocimiento de información. Escaneo y puertos de servicio. Comunicación entre dispositivos. Configuraciones de seguridad. Rutas de ataque.	Aplica los conocimientos teóricos en la práctica. Organiza y planifica. Analiza de información, deduce de procesos. Analiza y resuelve problemas. Creativo e innovador en el proceso de diseño y desarrollo de sistemas.	Compromiso con su formación personal y en su caso con el equipo de trabajo. Interés por aprender y trabajar. Tolerancia. Honestidad. Ética Profesional.
Módulo IV		

HACKEO ETICO E INGENIERIA SOCIAL

Competencia Específica

Identificar las técnicas de ingeniería social como vulnerabilidad de los sistemas para evitar amenazas informáticas que atenten contra la seguridad de la información.

Tipos de saberes

Saber (Conocimientos)	Saber hacer (Habilidades)	Saber ser (Actitudes y valores)
Métodos de búsqueda exploits. Tipos de ataque y tecnología (Hardware-software) que involucran. La Ingeniería Social y su clasificación.	Aplica los conocimientos teóricos en la práctica. Organiza y planifica. Analiza de información, deduce de procesos. Analiza y resuelve problemas. Creativo e innovador en el proceso de diseño y desarrollo de sistemas.	

Bibliografía básica

CEH v10 – Certified Ethical Hacker Study Guide
Ric Messier, Sybex
CEH v9 – Certified Ethical Hacker Study Guide
Sean-Philip Oriyano, Sybex
All in One CompTIA PenTest+ Certification Exam Guide
Ray Nutting, McGraw Hill

Bibliografía complementaria

INDICAR LA BIBLIOGRAFÍA NECESARIA, NO HAY UN NÚMERO MÁXIMO NI MÍNIMO; SE PUEDE INCLUIR DOCUMENTOS VIRTUALES

3.-Evaluación

Criterios de Evaluación (% por criterio)

Evaluación diagnóstica
INDICAR LOS INSTRUMENTOS RECOMENDABLES PARA LLEVAR A CABO ESTA EVALUACIÓN. NO TIENE UN VALOR PARA LA CALIFICACIÓN

Evaluación Formativa
INDICAR CUÁLES SON LOS PRODUCTOS RECOMENDADOS PARA LLEVAR A CABO LA EVALUACIÓN, PUEDEN INDICARSE POR MÓDULO.

Evaluación Sumativa
INDICAR CUÁLES SON LOS ASPECTOS O CRITERIOS A EVALUAR DETERMINANDO EL PORCENTAJE QUE LE CORRESPONDA AL CRITERIO, INCLUIR PORCENTAJE A LA AUTOEVALUACIÓN Y COEVALUACION.

4.-Acreditación

NO MODIFICAR

De acuerdo al **REGLAMENTO GENERAL DE EVALUACIÓN Y PROMOCIÓN DE ALUMNOS DE LA UNIVERSIDAD DE GUADALAJARA** que señala:

Artículo 5. El resultado final de las evaluaciones será expresado conforme a la escala de calificaciones centesimal de 0 a 100, en números enteros, considerando como mínima aprobatoria la calificación de 60. Las materias que no son sujetas a medición cuantitativa, se certificarán como acreditadas (A) o no acreditadas (NA).

Artículo 20. Para que el alumno tenga derecho al registro del resultado final de la evaluación en el periodo ordinario, establecido en el calendario escolar aprobado por el H. Consejo General Universitario, se requiere: I. Estar inscrito en el plan de estudios y curso correspondiente, y II. Tener un mínimo de asistencia del 80% a clases y actividades registradas durante el curso.

Artículo 25. La evaluación en periodo extraordinario se calificará atendiendo a los siguientes criterios: **I.** La calificación obtenida en periodo extraordinario, tendrá una ponderación del 80% para la calificación final; **II.** La calificación obtenida por el alumno durante el periodo ordinario, tendrá una ponderación del 40% para la calificación en periodo extraordinario, y **III.** La calificación final para la evaluación en periodo extraordinario será la que resulte de la suma de los puntos obtenidos en las fracciones anteriores.

Artículo 27. Para que el alumno tenga derecho al registro de la calificación en el periodo extraordinario, se requiere: I. Estar inscrito en el plan de estudios y curso correspondiente. II. Haber pagado el arancel y presentar el comprobante correspondiente. III. Tener un mínimo de asistencia del 65% a clases y actividades registradas durante el curso.

Artículo 33. El alumno que por cualquier circunstancia no logre una calificación aprobatoria en el periodo extraordinario, deberá repetir la materia en el ciclo escolar inmediato siguiente en que se ofrezca, teniendo la oportunidad de acreditarla durante el proceso de evaluación ordinario o en el periodo extraordinario, excepto para alumnos de posgrado.
En caso de que el alumno no logre acreditar la materia en los términos de este artículo, será dado de baja.

5.- Participantes en la elaboración

Código	Nombre

6.- Fecha de elaboración