Nombre del Módulo					
SEGURIDAD DE REDES					
MÓDULO	**Fecha de elaboración**			**Modalidad**	**Área de formación**
Módulo 3	DD	MM	AÑO	Curso	REDES
	14/12/2018				

PERFIL DEL DOCENTE
1. Formación: Contar con título profesional, grado de maestría en áreas afines a informática y computación. Tener dominio en el área de conocimiento de redes. Se recomienda que cuente con una certificación en redes. Cursos de formación docente. Comprensión de lectura en el idioma inglés. 2. Competencias: Comunicación oral y escrita, trabajo colaborativo y liderazgo, gestión de la información. 3. Habilidades: Manejo de grupo, pensamiento crítico, reflexivo y creativo, desarrollar estrategias o métodos de enseñanza y evaluación. 4. Experiencia: Con experiencia en el área y ámbito profesional, y además con experiencia en temas de seguridad informática y en el uso de herramientas de monitoreo y prevención de redes. 5. TICs: Conocimientos técnicos en el área de Redes de computadoras.

Propósito general:	**Presentación:**
Formar profesionistas con la capacidad para buscar, detectar y/o reparar vulnerabilidades en servidores WEB, Mediante distintas técnicas de ataque a servidores WEB teniendo en cuenta los conceptos de Hacking Ético.	En el módulo, el estudiante adquirirá los conocimientos teóricos y prácticos para la instalación, configuración y administración de un ecosistema virtual de pruebas para poder desarrollar las técnicas de ataque para buscar vulnerabilidades en servidores web y en caso de encontrar alguna vulnerabilidad, podrán poner en práctica las correcciones.

Proyecto Integrador del módulo / Reporte de Investigación
Configuración de un ecosistema virtual para realizar pruebas, realizado por equipos de 4 estudiantes.
Actividad Integradora del Módulo
Portafolio electrónico de evidencias de las actividades y prácticas realizadas

<table>
<tr><th>Nombre de la Subcompetencia</th><th>Elementos de la subcompetencia</th></tr>
<tr><td rowspan="4">1. Introducción a Hacking Ético

Número de semanas programadas

Semana No. 1 (Viernes/Sábado)

Propósito

El estudiante debe comprender los conceptos básicos del hacking ético para diferenciar entre los ataques maliciosos y los ataques éticos. Siguiendo este orden de ideas, el alumno creará un ecosistema virtual para realizar pruebas de las distintas técnicas de ataque buscando vulnerabilidades para poder corregirlas.</td><td>Conocimientos:

1.1. Hacking Ético
1.1.1 Fases de Hacking
1.1.2 Tipos de Hacking
1.1.3 Modalidades de Hacking
1.2 Instalación y configuración de Virtualizadores
1.2.1 Que es un Virtualizador
1.2.2 Instalación un Virtualizador
1.2.3 Configuración de Virtualizador
1.3 Creación de un Ecosistema Virtual
1.3.1 Instalación de una MV con Windows
1.3.2 Instalación de una MV con Kali Linux
1.3.3 Instalación de una MV con Metasploit</td></tr>
<tr><td>Habilidades:
Capacidad de aprender por cuenta propia
Pensamiento crítico
Determinación de soluciones y alternativas
Trabajo en equipo
Capacidad de análisis, síntesis y evaluación</td></tr>
<tr><td>Valores y actitudes profesionales:
Honestidad y Responsabilidad
Independencia
Trabajo Colaborativo</td></tr>
<tr><td colspan="2">Evidencias de desempeño</td></tr>
</table>

Rúbrica de prácticas (Laboratorios de Configuración de Ecosistema Virtual)		
Recursos didácticos	**Estrategia de Enseñanza**	**Estrategias de aprendizaje**
Apuntes Libro digital Presentaciones con diapositivas Ligas de bibliografía en internet	Discurso docente Practicas dirigidas	Mapas conceptuales Utilización de actividades de aprendizajes auténticos Resolución de problemas Debates.

Nombre de la Subcompetencia	**Elementos de la subcompetencia**
2 **Ataques.**	**Conocimientos:** **2.1 Recopilación de información.** 2.1.1 Google 2.1.2 Herramientas on-line 2.1.3 FOCA 2.1.4 whois **2.2 Escaneo de redes** 2.2.1 Escaneo de Protocolos de red 2.2.2 Escaneo de Vulnerabilidades **2.3 Explotación.** 2.3.1 Definición 2.3.2 Técnicas de Explotación 2.3.3 Acceso total
Número de semanas programadas	
Semana No. 2 (Viernes/Sábado)	
Propósito de la subcompetencia	
El estudiante analiza la infraestructura de red y pondrá en práctica las distintas técnicas de ataques éticos, iniciando con la recopilación de información necesaria para después realizar búsqueda de vulnerabilidades, en caso de encontrar realizar el ataque.	

	2.4 Post-Explotación 2.4.1 Definición de Post-Explotación 2.4.2 Incremento de privilegios en servidor 2.4.3 Obtención de contraseñas
	Habilidades: Determinación de soluciones y alternativas Trabajo en equipo Capacidad de análisis, síntesis y evaluación Solución de problemas
	Valores y actitudes profesionales: Honestidad y Responsabilidad Disciplina Independencia Trabajo Colaborativo

Evidencias de desempeño		
Rúbrica de prácticas (Laboratorios de ataques a servidor WEB montado dentro del ecosistema Virtual)		
Recursos didácticos	**Estrategia de Enseñanza**	**Estrategias de aprendizaje**
Apuntes Presentaciones con diapositivas Ligas de bibliografía en internet	Discurso docente Practicas dirigidas Prácticas de laboratorio	Mapas conceptuales Resolución de problemas

<table>
<tr><th>Nombre de la Subcompetencia</th><th>Elementos de la subcompetencia</th></tr>
<tr><td rowspan="5">3 Corrección de Vulnerabilidades

Número de semanas programadas

Semana No. 3 (Viernes/Sábado)

Propósito de la subcompetencia

El estudiante debe aplicar los conocimientos adquiridos para corregir las vulnerabilidades que fueron explotadas con el fin de configurar servidores WEB más seguros.</td><td>Conocimientos:

3.1 Escaneo de redes
3.1.1 Escaneo de Protocolos de red
3.1.2 Escaneo de Vulnerabilidades

3.2 Corrección de Vulnerabilidades
3.2.1 Análisis de Vulnerabilidad
3.2.2 Corrección de Vulnerabilidad

3.3 Explotación de Vulnerabilidades
3.3.1 Realizar pruebas de vulnerabilidades</td></tr>
<tr><td>Habilidades:
Determinación de soluciones y alternativas
Trabajo en equipo
Capacidad de análisis, síntesis y evaluación
Uso eficiente de la informática y las telecomunicaciones
Solución de problemas</td></tr>
<tr><td>Valores y actitudes profesionales:
Honestidad y Responsabilidad
Trabajo Colaborativo</td></tr>
<tr><td colspan="2">Evidencias de desempeño</td></tr>
<tr><td colspan="2">Rúbrica de prácticas
(Laboratorios de Corrección de Vulnerabilidades)</td></tr>
</table>

SEMINARIOS DE TITULACIÓN

Recursos didácticos	Estrategia de Enseñanza	Estrategias de aprendizaje
Apuntes Libro digital Presentaciones con diapositivas Ligas de bibliografía en internet	Discurso docente Practicas dirigidas Prácticas de laboratorio	Utilización de actividades de aprendizajes auténticos Resolución de problemas Debates.

Evaluación diagnóstica del Módulo:			
Instrumentos de diagnóstico	**Cuestionario de evaluación inicial** **Preguntas detonadoras**		
Evaluación Formativa:		**Evaluación Sumativa:**	
Competencias	**Instrumentos de Evaluación Formativa**	**Criterios de evaluación**	**Ponderación**
● **Introducción a Hacking Ético** ● **Ataques.** ● **Corrección de vulnerabilidades.**	**Rúbrica**	Comprensión del Hacking Ético y configuración de un Ecosistema virtual	**20%**
	Rúbrica	Búsqueda de vulnerabilidades, explotación y post-explotación.	**30%**
	Rúbrica	Búsqueda y corrección de vulnerabilidades	**30%**
		Reporte de Investigación	**20%**
		Total=	**100%**

BIBLIOGRAFÍA

Básicas:	Complementarias:
Bibliográficas:	Bibliográficas:
Karina Astudillo (2016). "**Hacking Ético 101**". Editorial Createspace Independent Publishing Platform.	
Ligas de Internet:	Ligas de Internet:
Videos:	
Curso Online de Hacking Ético **https://www.udemy.com/hacking-etico-de-cero-a-cien/learn/v4/overview** **Curso Online de Hacking Web y Pentesting** **https://www.udemy.com/aprenda-hacking-web-y-pentesting/learn/v4/content**	

Mtro. Erwin Bermúdez Casillas
Instructor del Módulo III

Mtro. Aron de la Cruz Vázquez
Coordinador del Seminario de Titulación