PLAN DE TRABAJO

I. Datos de la institución

Plantel	UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN DIVISIÓN SISTEMA UNIVERSIDAD ABIERTA Y EDUCACIÓN A DISTANCIA Modalidad: A Distancia	**Grado o Licenciatura**	Licenciatura en Informática

II. Datos del asesor

Nombre	RAMIREZ CHAVERO ESTHER	**Correo**	echavero@comunidad.unam.mx

III. Datos de la asignatura

Nombre	HACKEO ÉTICO	**Clave**	0553	**Grupo**	8891
Modalidad	Optativa	**Plan**	2012	**Fecha de inicio del semestre**	04 de febrero de 2025
Horas de asesoria semanal	4	**Horario**	Martes: 09:00 - 11:00 hrs Jueves: 09:00 - 11:00 hrs	**Fecha de término del semestre**	13 de junio de 2025

IV. Contenido temático

TEMA	HORAS		
	Total	**Teoría**	**Práctica**
I. Sistemas Detectores de intrusos	6	6	0
II. Firewalls y Honeypots	6	6	0

III. El hackeo ético	6	6	0
IV. Ciclo del hackeo	4	4	0
V. Protocolos seguros	10	10	0
VI. Tipo de ataques en redes	10	10	0
VII. Bastiones y Zona Desmilitarizada	4	4	0
VIII. Proxys	4	4	0
IX. VPNs	4	4	0
X. Introducción a la seguridad en redes inalámbricas	6	6	0
XI. Voz sobre IP	4	4	0

V. Presentación general del programa

Seré tu asesora durante el presente semestre, la forma en que trabajaremos será por medio de la plataforma, por tal motivo te solicito que para conocer de manera pertinente las actividades que debes realizar por unidad descargues el plan de trabajo.

Están establecidas 2 sesiones por semana de 2 horas de chat con (4 horas por semana), en caso de que te surja alguna duda puedes conectarte, esta conexión no es obligatoria para ti, sin embargo yo estaré a lo largo del semestre en los días y horarios establecidos. También nos podemos comunicar por: correo y mensajería de la plataforma.

Contaremos con las siguientes sesiones de videoconferencia:

1. Sesión 1: 6 de febrero / 09:00 a 11:00 h. / dudas de la unidad 1, 2 y 3
2. Sesión 2: 27 de marzo / 09:00 a 11:00 h. / dudas de la unidad 4, 5 y 6
3. Sesión 3: 24 de abril / 09:00 a 11:00 h. / dudas de la unidad 7, 8 y 9
4. Sesión 4: 20 de mayo / 09:00 a 11:00 h. / dudas de la unidad 10 y 11

VI. Forma en que el alumno deberá preparar la asignatura

Revisaré tus actividades de aprendizaje y tendrás una retroalimentación a cada una de ellas en un tiempo no mayor a 72 horas hábiles. En caso de que sean entregadas de forma extemporánea, es muy probable que tarde más en revisarlas. No dejes de preguntar cuanto sea necesario y las veces que consideres pertinentes vía correo, mensajería o chat. En caso de que necesites volver a elaborar una actividad, ésta se evaluará sobre 9 (nueve).

Puedes entregar tus actividades fuera de la fecha indicada, revisaré tus actividades, solo que las que se entregan de forma extemporánea, es posible que me tarde un poco más en calificarlas.

No debes copiar y pegar información de Internet, en caso de que lo hagas tu calificación será 0 (cero).

CALENDARIO DE ACTIVIDADES

Fecha de entrega	No. Unidad	No. Actividad	Descripción de la de actividad de acuerdo a la plataforma	Ponderación
20 de febrero de 2025	UNIDAD 1: Sistemas Detectores de intrusos	Act. de aprendizaje 1	Responde las siguientes preguntas 1. ¿Cuáles son los principales tipos de ataques que detectan los IDS? 2. ¿Cómo se diferencia un IDS de un IPS? 3. ¿Cuáles son los principales desafíos en la implementación de un IDS? 4. ¿Qué factores se deben considerar al seleccionar un IDS? 5. ¿Cómo se evalúa la eficacia de un IDS?	5 %
27 de febrero de 2025	UNIDAD 1: Sistemas Detectores de intrusos	Act. de aprendizaje 2	Elaborar un informe sobre las mejores prácticas para la implementación y gestión de un IDS.	5 %
06 de marzo de 2025	UNIDAD 2: Firewalls y Honeypots	Act. de aprendizaje 1	Elaborar un informe sobre las mejores prácticas para la implementación y gestión de firewalls y honeypots.	5 %
13 de marzo de 2025	UNIDAD 2: Firewalls y Honeypots	Act. de aprendizaje 2	Responde las siguientes preguntas. 1. ¿Cuáles son las principales diferencias entre un firewall de estado y uno de próxima generación? 2. ¿Qué tipos de honeypots existen y cuáles son sus ventajas y desventajas? 3. ¿Cómo se puede utilizar un honeypot para recopilar inteligencia sobre amenazas? 4. ¿Cuáles son los principales desafíos en la implementación de un firewall? 5. ¿Cómo se puede integrar un honeypot en una estrategia de seguridad más amplia?	5 %
20 de marzo de 2025	UNIDAD 3: El hackeo ético	Act. de aprendizaje 1	Responde las siguientes preguntas 1. ¿Cuál es la diferencia entre un hacker blanco, un hacker gris y un hacker negro? 2. ¿Cuáles son las principales fases de una prueba de penetración? 3. ¿Qué es un exploit y cómo se crea? 4. ¿Cuáles son las últimas tendencias en seguridad cibernética?	4 %
25 de marzo de 2025	UNIDAD 4: Ciclo del hackeo	Act. de aprendizaje 1	Responde las siguientes preguntas 1. ¿Cuál es la diferencia entre un ataque activo y un ataque pasivo? 2. ¿Qué es un exploit y cómo se utiliza? 3. ¿Cuáles son las principales técnicas de ingeniería social? 4. ¿Cómo se puede proteger un sistema de un ataque de ransomware? 5. ¿Qué es un botnet y cómo se utiliza en los ciberataques?	5 %

27 de marzo de 2025	UNIDAD 5: Protocolos seguros	Act. de aprendizaje 1	Responde las siguientes preguntas: 1. ¿Cuál es la diferencia entre un protocolo de transporte y un protocolo de aplicación? 2. ¿Qué es un certificado digital y para qué sirve? 3. ¿Cuáles son los principales tipos de ataques a protocolos de seguridad? 4. ¿Cómo se puede garantizar la confidencialidad, integridad y autenticidad de los datos transmitidos a través de una red? 5. ¿Qué es una VPN y cómo funciona?	5 %
03 de abril de 2025	UNIDAD 5: Protocolos seguros	Act. de aprendizaje 2	Realiza una investigación de los tipos de ataques más comunes a los protocolos de seguridad (Man-in-the-middle, inyección SQL, etc.).	6 %
10 de abril de 2025	UNIDAD 6: Tipo de ataques en redes	Act. de aprendizaje 1	Responde las siguientes preguntas 1. ¿Cuál es la diferencia entre un ataque activo y un ataque pasivo? 2. ¿Qué es un ataque de denegación de servicio (DDoS)? 3. ¿Cómo se puede proteger contra ataques de phishing? 4. ¿Cuáles son las últimas tendencias en ataques cibernéticos? 5. ¿Qué es un exploit y cómo se crea?	5 %
22 de abril de 2025	UNIDAD 7: Bastiones y Zona Desmilitarizada	Act. de aprendizaje 1	Responde las siguientes preguntas 1. ¿Cuál es la diferencia entre un bastión físico y un bastión lógico? 2. ¿Qué tipo de servicios se suelen colocar en una DMZ? 3. ¿Cuáles son los principales riesgos asociados a los bastiones y DMZ? 4. ¿Cómo se puede proteger un bastión de ataques? 5. ¿Qué medidas de seguridad se deben implementar en una DMZ?	5 %
24 de abril de 2025	UNIDAD 8: Proxys	Act. de aprendizaje 1	Responde las siguientes preguntas 1. ¿Cuál es la diferencia entre un proxy transparente y un proxy anónimo? 2. ¿Qué es un proxy inverso y para qué se utiliza? 3. ¿Cuáles son los principales riesgos asociados a los proxys? 4. ¿Cómo se puede proteger un proxy de ataques? 5. ¿Qué medidas de seguridad se deben implementar en un proxy?	5 %
06 de mayo de 2025	UNIDAD 9: VPNs	Act. de aprendizaje 1	Responde las siguientes preguntas 1. ¿Cuál es la diferencia entre una VPN basada en IPSec y una VPN basada en SSL/TLS? 2. ¿Qué es un túnel VPN y cómo se establece? 3. ¿Cuáles son los principales riesgos asociados a las VPNs? 4. ¿Cómo se puede proteger una VPN de ataques? 5. ¿Qué medidas de seguridad se deben implementar en una VPN?	5 %
13 de mayo de 2025	UNIDAD 10: Introducción a la seguridad en redes inalámbricas	Act. de aprendizaje 1	Responde las siguientes preguntas 1. Cuál es la diferencia entre WEP, WPA y WPA2? 2. ¿Qué es un ataque de deauth y cómo funciona? 3. ¿Cómo se puede proteger una red inalámbrica de ataques de fuerza bruta? 4. ¿Qué es un punto de acceso malicioso y cómo se puede detectar? 5. ¿Qué medidas de seguridad se deben implementar en una red inalámbrica?	5 %

20 de mayo de 2025	UNIDAD 11: Voz sobre IP	Act. de aprendizaje 1	Responde las siguientes preguntas 1. Cuál es la diferencia entre VoIP y la telefonía tradicional? 2. ¿Qué es el protocolo SIP y cuál es su función en VoIP? 3. ¿Cuáles son los principales desafíos de calidad en las llamadas VoIP? 4. ¿Cómo se puede asegurar la privacidad en las comunicaciones VoIP? 5. ¿Qué futuro le ves a la tecnología VoIP?	5 %

VII. Sistema de evaluación

FACTORES	DESCRIPCIÓN	
Requisitos	Deberás elaborar las actividades solicitadas en el plan de trabajo, así como realizar un examen final al finalizar el semestre, si no realizas el examen, no puedes acreditar la asignatura.	
Porcentajes	Act. de aprendizaje Examen(es) TOTAL	70 % 30 % 100 %

La calificación final de la asignatura está en función de la ponderación del asesor, no de la que se visualiza en la plataforma. Es necesario solicitar por correo electónico la calificación final al asesor.

VIII. Recursos y estratégias didácticas

Lecturas Obligatorias	(X)
Trabajos de Investigación	(X)
Elaboración de Actividades de Aprendizaje	(X)
Videos	(X)
Plataforma Educativa	(X)
Chat	(X)
Sitios de Internet	(X)
Plan de Trabajo	(X)