INSTITUTO POLITÉCNICO NACIONAL
SECRETARIA ACADÉMICA
DIRECCIÓN DE EDUCACION MEDIA SUPERIOR
CENTRO DE ESTUDIOS CIENTÍFICOS Y TECNOLÓGICOS No. 13
"RICARDO FLORES MAGÓN"

G U Í A

d e e s t u d i o p a r a
presentar ETS de la
UNIDAD DE APRENDIZAJE
PRUEBAS DE PENETRACIÓN
Semestre 2026-2
TURNO VESPERTINO

Integrantes de la academia: **Alfredo Campos Guerrero**

Fecha de Elaboración: **13/05/2026**

FORMATO DE LA GUÍA DE ESTUDIO

Área:	Nombre de la Unidad de Aprendizaje:	Nivel/semestre:
Tecnológica	**Pruebas de Penetración**	**Sexto**

Instrucciones generales de la guía:

Anotar aspectos que el alumno debe considerar antes de presentar el examen:

- Esta guía no tiene ningún valor sobre la calificación final

Presentación:

Esta Unidad de Aprendizaje contribuye a conocer las diferentes técnicas y enfoques de Pruebas de Penetración a Sistemas Informáticos llamado en inglés "Pentesting" para su implementación y gestión en las organizaciones, aplicando las normas, técnicas y estándares nacionales e internacionales, así como mantener actualizadas las tecnologías de la información y comunicación enfocadas a la seguridad de sistemas y redes informáticas. Introduce al estudiante para que cuente con una visión de los modelos para tomar responsablemente decisiones sobre qué norma, estándar o técnica aplicar de acuerdo con las formas y usos que se esté aplicando en la organización

Objetivos

Los principales objetos del conocimiento que se adquirirán y serán cuerpo de las acciones o desempeños a realizar son:

- Conocer las herramientas que se utilizan para realizar el Pentesting
- Saber configurar e instalar máquinas virtuales
- Conocer el Sistema Operativo Linux
- Conocer las redes de datos LAN, MAN y WAN

Justificación

Las competencias profesionales (generales y particulares) implican como principales objetos de conocimiento de las redes de datos por medio de las bases metodológicas, que podrá vincular con su entorno socioeconómico y laboral. Asimismo, en la particularidad del estudiante:

- Instala y pone en operación un laboratorio de Pentesting
- Sabe ejecutar comandos de Linux y tener el conocimiento necesario de redes.

Estructura y contenidos

1. Identifica los elementos y características de las pruebas de penetración a sistemas de seguridad de la información para reducir el impacto de vulnerabilidades dentro de una organización con base a la normatividad vigente.
   1.1 Conoce los fundamentos de las pruebas de penetración en sistemas informáticos dentro de una organización para reducir el impacto de vulnerabilidades de acuerdo con la normatividad vigente.
   1.2 Reconoce los tipos de pruebas de penetración que existen en los sistemas informáticos para seleccionar la estrategia a seguir y reducir la vulnerabilidad dentro de una organización con base a la normatividad vigente.

2. Diseña el procedimiento de las pruebas de penetración para la implementación en un escenario controlado bajo la normatividad vigente.
   2.1 Comprende las diversas metodologías para realizar un "pentesting" Identificando los modelos de amenazas existentes para vulnerar un sistema de manera controlada, bajo la normatividad vigente.
   2.2 Distingue los procesos para llevar a cabo la explotación del sistema, utilizando técnicas y/o herramientas adecuadas a la vulnerabilidad y bajo la normatividad vigente
   2.3 Define los procedimientos para realizar un análisis de vulnerabilidades adecuados a la organización y bajo la normativa vigente

3. Implementa pruebas de penetración en escenarios controlados para identificar vulnerabilidades bajo la normatividad vigente.
   3.1 Emplea técnicas para la explotación en diversos Sistemas Operativos bajo un entorno seguro y Controlado
   3.2 Explica los exploits más adecuados de acuerdo a la vulnerabilidad o ataque que se pretende prevenir de acuerdo al análisis pertinente
   3.3 Genera reportes de las vulnerabilidades identificadas por medio del pentesting para que la organización tome acciones pertinentes a favor de su seguridad de la información, bajo la normatividad vigente.

Materiales para la elaboración de la guía

No Aplica

Actividades de estudio

- Conoce la definición de Pruebas de penetración (Pentesting).
- Identifica los tipos de vulnerabilidades. ● Distingue los diferentes tipos de malware.
- Reconoce los diversos ataques. ● Identifica los actores que intervienen en un "pentesting"
- Normativa relacionada con "pentesting" ● Conoce los tipos de tipos de Pentesting (hackers) o Pentesting de caja blanca − Objetivos y funciones o Pentesting de caja gris − Objetivos y funciones o Pentesting de caja negra. − Objetivos y funcione
- Conoce que es un entorno controlado en una organización. o Grados de conocimiento o Caja blanca, gris y negra.
- Identifica la organización jerárquica de la organización para llevar a cabo un pentesting. o Administración del recurso humano encargado del pentesting o Pentestings Internos y externos. o Ventajas y desventajas. ● Importancia del departamento de ciberseguridad en la organización
- Diferencia los Tipos de metodologías para el "pentesting" ○ Metodologías vigentes.
- Metodologías de Escaneo:
    - Fases
    - Procedimiento ○ Ventajas y desventajas.

  ● Explica los Modelos de amenazas en los sistemas informáticos.
  ● Exploits
  ● Shells (directo y reverso)
  ● Payloads
  ● Metasploits

- Conoce las diversas técnicas de explotación.
- Identifica los procedimientos para análisis de vulnerabilidades.
    - Análisis de vulnerabilidades.
    - Procedimientos

- Analiza las técnicas de explotación:
    - Explotación en Windows.
    - Introducción a Linux
    - Programación o Estructura general de un programa o Comandos básicos
- Conoce los tipos de reportes de vulnerabilidades.
- Desglose de vulnerabilidades encontradas o Propuestas de mitigación.

Información Adicional

- Ninguna

Bibliografía Básica

- Instalación Y Mantenimiento De Servicios De Redes locales. Autor: Francisco Molina. Edit. AlfaOmega
- Sistema Operativo Linux. Autor: Francisco Molina. Edit. AlfaOmega
- Sistemas Informáticos Multiusuario y en Red. Autor: Laura Raya. Edit. Anaya Multimedia
- Construye y Configura Tu Red. Autor: Rosenda Hernández. Edit. Anaya Multimedia

Guía de estudio

Temas teóricos:

- Defina 3 tipos de hackers que se encuentran en el internet y sus características de cada uno
- Definición de activo informático
- Definición de amenaza
- Definición de vulnerabilidad
- Definición de Exploit y payload
- Cuales son los servicios de Ethical Hacking
- Actividades realizadas en la etapa de Reconocimiento en una Prueba de penetración
- Actividades realizadas en la etapa de Enumeración en una Prueba de penetración
- Actividades realizadas en la etapa de Análisis de Vulnerabilidades en una Prueba de penetración
- Actividades realizadas en la etapa de Explotación en una Prueba de penetración
- **Menciona para que sirve la herramienta de NMAP**
- **Menciona para que sirve la herramienta de DNSDumpster**
- **Menciona para que sirve la herramienta msfconsole**
- Define que es Google Hacking
- Define que es OSINT
- Define que es Recolección de DNS
- Define que es Geolocalización
- Define que es huella digital
- Define que es Inyección SQL
- Define que es baiting
- Define que es Web Spoofing
- Define que es Denegación de Servicios
- Define que es Phishing

Examen práctico

1) **Podemos realizar este hackeo utilizando el concepto de MitM (Man-in-the-Middle)**
   a) Abrimos 3 equipos virtuales:

- Metasploit2 (Servidor Web vulnerable) con el usuario msfadmin y la misma contraseña
- Metasploi3-workspace-win2k8 (Servidor con Windows 2008) con el usuarios Vgrant y la misma contraseña
- Kali Linux (máquina atacante)

Podemos hacer uso de la herramienta Ettercap para la captura de usuario y contraseña entre la Metasploit2 y Metaesploit3. En su caso, también podemos hacer uso del WireShark (snnifer)

2) Escaneo de una red con NMAP con escaneo de puertos con UDP y TCP, ejecutados desde Kali Linux, como posible hacker dentro de una red, haciendo uso de las máquinas virtuales.