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 a Sistemas Informaticos.

CICLO ESCOLAR 2026-2

TURNO Matutino

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

Presidente de academia: Lic. Octavio Tapia Rodríguez **Fecha de Elaboración: Abril 2026**

Área:	**Nombre de la Unidad de Aprendizaje:**	**Nivel/semestre:**
Tecnológica	**Prueba de Penetración a Sistemas Informáticos**	**6°**

Instrucciones generales de la guía:

- La guía tiene no tiene valor.

Para revisión del examen:

- El alumno deberá solicitar el formato de revisión de examen en el área Tecnológica.
- Lo anterior deberá realizarse en plazo no mayor a 48 horas a partir de que se le notifico la calificación correspondiente.

Presentación:

La presente guía de estudio, permitirá al estudiante el desarrollo de habilidades y competencias en las pruebas de Pentesting.

Objetivos

Contribuir 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.

Justificación

Preparar al estudiante para que desarrolle competencias y habilidades en pruebas de Pentesting.

Estructura y contenidos

- **UNIDAD 1: Introducción al Pentesting.**

  1.1 ¿Qué es el Pentesting?
  1.2 Tipos de Vulnerabilidades
  1.3 Tipos de Malware
  1.4 Tipos de Ataques
  1.5 Actores del Pentesting
  1.6 Tipos de Pentesting
  1.7 Normatividad y Ética
  1.8 Entornos Controlados
  1.9 Pentesting Interno vs Externo

- **UNIDAD 2: METODOLOGÍA DEL PENTESTING**

  2.1 Metodologías de Pentesting
  2.2 Fases del Pentesting
  2.3 Modelos de Amenazas
  2.4 Técnicas de Explotación
  2.5 Herramientas de Pentesting
  2.6 Análisis de Vulnerabilidades

- **UNIDAD 3: IMPLEMENTACIÓN DEL PENTESTING**

  3.1 Sistemas Operativos
  3.2 Linux Básico
  3.3 Programación Básica
  3.4 Tipos de Exploits
  3.5 Uso de Herramientas
  3.6 Reporte de Vulnerabilidades

Evaluación

Materiales para la elaboración de la guía

No Aplica

Actividades de estudio

- Computadora de preferencia con Windows 10 o superior.
- Internet
- Software para llevar a cabo practicas de Pentesting

Información adicional

Software para elaborar pruebas de Pentesting

Integrantes de la academia

Lic. Octavio Tapia Rodríguez

Índice de Contenidos

I. PARTE TEÓRICA

- **UNIDAD 1: Introducción al Pentesting.**

1.1 ¿Qué es el Pentesting?

El pentesting (pruebas de penetración) es una técnica de ciberseguridad que consiste en simular ataques reales a sistemas informáticos con el fin de identificar vulnerabilidades antes de que sean explotadas por atacantes maliciosos.

Objetivos:

- Detectar fallas de seguridad
- Evaluar el nivel de protección de un sistema
- Proponer soluciones para mitigar riesgos

El pentesting debe realizarse en entornos controlados y con autorización, ya que de lo contrario es ilegal.

1.2 Tipos de Vulnerabilidades

Las vulnerabilidades son debilidades en un sistema.

Tipos principales:

1. Vulnerabilidades de sistema
Fallas en el sistema operativo (Windows, Linux)
Ejemplo: versiones desactualizadas

2. Vulnerabilidades de aplicación
Errores en software o aplicaciones web
Ejemplo: inyección SQL

3. Vulnerabilidades de red
Configuraciones incorrectas de red
Puertos abiertos innecesarios

1.3 Tipos de Malware

El malware es software malicioso diseñado para dañar o explotar sistemas.

Tipos:

- Virus: se propaga infectando archivos
- Troyano: se oculta como software legítimo
- Ransomware: secuestra información
- Spyware: roba información

1.4 Tipos de Ataques

Principales ataques:

- Fuerza bruta: intenta múltiples contraseñas
- Ingeniería social: manipula a personas
- Ataques de red: interceptación de datos
- Inyección SQL: manipulación de bases de datos

1.5 Actores del Pentesting

- Pentester: experto en seguridad
- Organización: sistema evaluado
- Equipo de ciberseguridad: supervisa
- Cliente: solicita el servicio

1.6 Tipos de Pentesting

- Caja Blanca
  - Acceso completo al sistema
  - Más rápido y detallado
- Caja Gris
  - Acceso parcial
  - Simula usuario interno
- Caja Negra
  - Sin información previa
  - Simula un atacante real

1.7 Normatividad y Ética

- El pentesting debe cumplir:
- Autorización legal
- Contrato firmado
- Uso ético de la información

Sin esto, se considera delito informático.

1.8 Entornos Controlados

- Son ambientes donde se realizan pruebas sin afectar sistemas reales.
  Ejemplos:
  - Máquinas virtuales
  - Redes simuladas
  - Laboratorios
  - Ventajas:
  - Seguridad
  - Repetición de pruebas
  - Sin riesgo real

1.9 Pentesting Interno vs Externo

- Interno:
  Simula ataque desde dentro
  Evalúa empleados o accesos internos

- Externo:
  Simula ataque desde internet
  Evalúa seguridad perimetral

• UNIDAD 2: METODOLOGÍA DEL PENTESTING

2.1 Metodologías de Pentesting

- Son procedimientos estructurados para realizar pruebas.
  Ejemplo:
  - OWASP
  - Importancia:
  - Orden
  - Repetibilidad
  - Estandarización

2.2 Fases del Pentesting

1. Reconocimiento

    Recolección de información
    Ejemplo: direcciones IP, dominios

2. Escaneo

    Identificación de puertos abiertos
    Servicios activos

3. Explotación

    Uso de vulnerabilidades para acceder

4. Post-explotación

    Escalada de privilegios
    Persistencia

5. Reporte

    Documentación de hallazgos

2.3 Modelos de Amenazas

- Permiten identificar riesgos potenciales.
    Elementos:
    - Exploit: Código que aprovecha una vulnerabilidad.
    - Payload: Carga maliciosa que se ejecuta.
    - Shell
        Acceso remoto:
            Directo
            Reverso
    - Framework
        Ejemplo: Metasploit

2.4 Técnicas de Explotación

- Local
  Requiere acceso previo

- Remoto
  Se realiza desde fuera del sistema

2.5 Herramientas de Pentesting

- Kali Linux
  Sistema operativo especializado

- Metasploit
  Framework para explotación

- Nessus
  Escáner de vulnerabilidades

- FOCA
  Análisis de metadatos

2.6 Análisis de Vulnerabilidades

- Proceso para detectar fallas.
  Pasos:
  - Identificar vulnerabilidades
  - Analizar impacto
  - Priorizar riesgos
  - Documentar

- **UNIDAD 3: IMPLEMENTACIÓN DEL PENTESTING**

3.1 **Sistemas Operativos**

- Windows
  Uso común en empresas
- Linux
  Más usado en seguridad

3.2 Linux Básico

- Comandos importantes:
  - ls → listar archivos
  - cd → cambiar directorio
  - pwd → ruta actual
  - chmod → permisos
  - apt-get → instalar software

3.3 Programación Básica

- Estructura:
- Entrada
- Proceso
- Salida
- Uso:
- Automatización
- Scripts de ataque

3.4 Tipos de Exploits

- Locales
- Remotos
- Día cero
- Activos
- Pasivos

3.5 Uso de Herramientas

- Metasploit
- Ejecuta exploits
- Genera accesos
- Nessus
- Escanea vulnerabilidades
- Genera reportes

3.6 Reporte de Vulnerabilidades

- Documento final del pentesting.
- Debe incluir:
- Introducción
- Alcance
- Metodología
- Vulnerabilidades encontradas
- Evidencias
- Nivel de riesgo
- Recomendaciones

Preguntas de Opción Múltiple

1. ¿Qué es el pentesting?
A) Un ataque ilegal
B) Un análisis de datos
C) Una simulación de ataques controlados
D) Un antivirus

2. ¿Cuál es el objetivo principal del pentesting?
A) Destruir sistemas
B) Detectar vulnerabilidades
C) Crear malware
D) Aumentar velocidad

3. ¿Qué es una vulnerabilidad?
A) Un virus
B) Un firewall
C) Un software seguro
D) Una debilidad en un sistema

4. ¿Cuál es un tipo de vulnerabilidad?
A) De Sistema
B) Lógica
C) Fisica
D) Virtual

5. ¿Qué tipo de malware secuestra información?
A) Virus
B) Spyware
C) Ransomware
D) Gusano

6. ¿Qué ataque intenta múltiples contraseñas?
A) Phishing
B) Fuerza bruta
C) MITM
D) DoS

7. ¿Quién realiza el pentesting?
A) Pentester
C) Hacker ilegal
D) Programador
A) Usuario

8. ¿Qué implica la ética en pentesting?
A) Atacar sin permiso
B) Uso legal y autorizado
C) Robo de datos
D) Espionaje

9. ¿Qué es malware?
A) Software útil
B) Red
C) Sistema operativo
D) Software malicioso

10. ¿Qué es ingeniería social?
A) Ataque técnico
B) Virus
C) Manipulación de personas
D) Firewall

11. ¿Qué es pentesting de caja blanca?
A) Sin información
B) Acceso total
C) Acceso externo
D) Ataque físico

12. ¿Caja negra significa?
A) Acceso total
B) Acceso parcial
C) Sin información previa
D) Sistema cerrado

13. ¿Caja gris implica?
A) Sin acceso
B) Acceso parcial
C) Acceso total
D) Sin pruebas

14. ¿Pentesting interno simula?
A) Ataque externo
B) Virus
C) Red pública
D) Ataque desde dentro

15. ¿Pentesting externo evalúa?
A) Seguridad perimetral
B) Usuarios internos
C) Hardware
D) Software

16. ¿Qué es un entorno controlado?
A) Sistema real
B) Laboratorio seguro
C) Red pública
D) Internet

17. ¿Qué herramienta crea entornos controlados?
A) Antivirus
B) Navegador
C) Editor
D) VirtualBox

18. ¿Qué es una máquina virtual?
A) Sistema simulado
B) Red
C) Hardware físico
D) Servidor real

19. ¿Qué evita un entorno controlado?
A) Ataques
B) Virus
C) Errores
D) Daños a sistemas reales

20. ¿Qué se requiere para pentesting legal?
A) Internet
B) Software
C) Autorización
D) Antivirus

21. ¿Primera fase del pentesting?
A) Explotación
B) Reporte
C) Reconocimiento
D) Escaneo

22. ¿Qué se hace en el escaneo?
A) Atacar
B) Buscar vulnerabilidades
C) Reportar
D) Borrar datos

23. ¿Qué fase usa exploits?
A) Reconocimiento
B) Explotación
C) Reporte
D) Análisis

24. ¿Qué ocurre en post-explotación?
A) Inicio
B) Escaneo
C) Instalación
D) Control del sistema

25. ¿Qué es un exploit?
A) Código que explota vulnerabilidad
B) Sistema
C) Red
D) Virus

26. ¿Qué es un payload?
A) Sistema
B) Carga maliciosa
C) Red
D) Firewall

27. ¿Qué es un shell?
A) Sistema
B) Virus
C) Acceso remoto
D) Hardware

28. ¿Qué es Metasploit?
A) Antivirus
B) Sistema operativo
C) Red
D) Framework de explotación

29. ¿Qué es Nmap?
A) Escáner de red
B) Firewall
C) Virus
D) Editor

30. ¿Qué identifica Nmap?
A) Usuarios
B) Puertos y servicios
C) Archivos
D) Programas

31. ¿Qué es Kali Linux?
A) Antivirus
B) Red
C) Software común
D) Sistema operativo de pentesting

32. ¿Qué herramienta explota vulnerabilidades?
A) Nmap
B) Wasp
C) Nessus
D) Metasploit

33. ¿Qué herramienta escanea vulnerabilidades?
A) Metasploit
B) Nessus
C) Paint
D) Chrome

34. ¿Comando para escaneo básico?
A) nmap -sV
B) ls
C) cd
D) ping

35. ¿Comando para abrir Metasploit?
A) nmap
B) apt
C) msfconsole
D) sudo

36. ¿Comando para listar archivos?
A) cd
B) pwd
C) rm
D) ls

37. ¿Comando para cambiar directorio?
A) ls
B) cd
C) pwd
D) nano

38. ¿Comando para ver IP?
A) IP a
B) ls
C) cd
D) rm

39. ¿Comando para probar conexión?
A) ping
B) ls
C) cd
D) chmod

40. ¿Qué hace apt-get?
A) Elimina archivos
B) Instala software
C) Borra sistema
D) Escanea red

41. Si un puerto 21 está abierto, ¿qué servicio es?
A) HTTP
B) SSH
C) DNS
D) FTP

42. ¿Puerto 22 corresponde a?
A) SSH
B) FTP
C) HTTP
D) SMTP

43. ¿Puerto 80 es?
A) FTP
B) SSH
C) DNS
D) HTTP

44. ¿Qué indica puerto abierto?
A) Error
B) Servicio activo
C) Virus
D) Firewall

45. ¿Qué riesgo tiene Telnet?
A) Seguro
B) Rápido
C) No cifrado
D) Moderno

46. ¿Qué indica acceso root?
A) Control total
B) Usuario básico
C) Sin acceso
D) Error

47. ¿Qué comando muestra usuario actual?

A) ls

B) whoami

C) cd

D) pwd

48. ¿Qué comando muestra sistema?

A) uname -a

B) ls

C) cd

D) rm

49. ¿Qué debe incluir un reporte?

A) Errores

B) Sugerencias

C) Vulnerabilidades

D) Comandos

50. ¿Qué se recomienda tras detectar vulnerabilidad?

A) Ignorar

B) Borrar sistema

C) Apagar red

D) Mitigar

51. SQL Injection afecta:

A) Red

B) Base de datos

C) CPU

D) RAM

52. XSS afecta:

A) Servidor

B) Red

C) Hardware

D) Cliente

53. Buffer overflow permite:
A) Ejecución de código
B) Velocidad
C) Red
D) Firewall

54. Zero-day es:
A) Antigua
B) Reparada
C) Conocida
D) Desconocida

55. Contraseña débil implica:
A) Seguridad
B) Red
C) Vulnerabilidad
D) Sistema

56. Servicio innecesario implica:
A) Seguridad
C) Rendimiento
D) Velocidad
B) Riesgo

57. Puertos abiertos implican:
A) Seguridad
B) Red
C) Superficie de ataque
D) Hardware

58. IDS detecta:
A) Ataques
B) Hardware
C) Red
D) CPU

59. IPS hace:
A) Detecta
B) Bloquea
C) Red
D) CPU

60. SSH ofrece:

A) Acceso seguro
B) Red
C) CPU
D) RAM

II. PARTE PRACTICA

- Máquina Virtual
  - Crear entorno seguro
- Sistemas Operativos
  - Instalación de MV
- Kali Linux
  - Instalación
  - Configuración completa
- Configurar Red
  - Modo NAT
  - Modo RED INTERNA
- Comandos Linux
  - Uso práctico
- Pruebas de Pentesting
  - Identificar IP
  - Escaneo con Nmap
  - Escaneo de vulnerabilidades
- Explotación con Metasploit
  - Ejecución de exploits
  - Buscar exploits
  - Ejecución de exploits
  - Post-explotación
  - Reporte

- Nmap

  Escaneo y reporte

- Resultados

  Puertos abiertos
  Vulnerabilidades

- Evidencias

  Capturas de Pantalla

Bibliografía básica

- Raphaël RAULT, Laurent SCHALKWIJK, ACISSI, Marion AGÉ, Nicolas CROCFER, Robert CROCFER, David DUMAS, Franck EBEL, Guillaume FORTUNATO, Jérôme HENNECART, Sébastien LASSON. (2018). Seguridad informática - Hacking Ético Conocer el ataque para una mejor defensa. Barcelona: ENI.
- Georgia Weidman. (2014). Penetration Testing: A Hands-On Introduction to Hacking.
- Solomongo CEH. (2022). ANALISIS DE VULNERABILIDADES: Riesgos y Amenazas. España: Solomongo.
- Jim O'Gorman, Mati Aharoni, Raphaël Hertzog. (2021). Kali Linux Revealed: Mastering the Penetration Testing Distribution.

Integrantes de la academia

Lic. Octavio Tapia Rodríguez