

COMPTIA · PLUS SERIES

VERSIÓN 3

CompTIA PenTest+ V3

Examen PT0-003

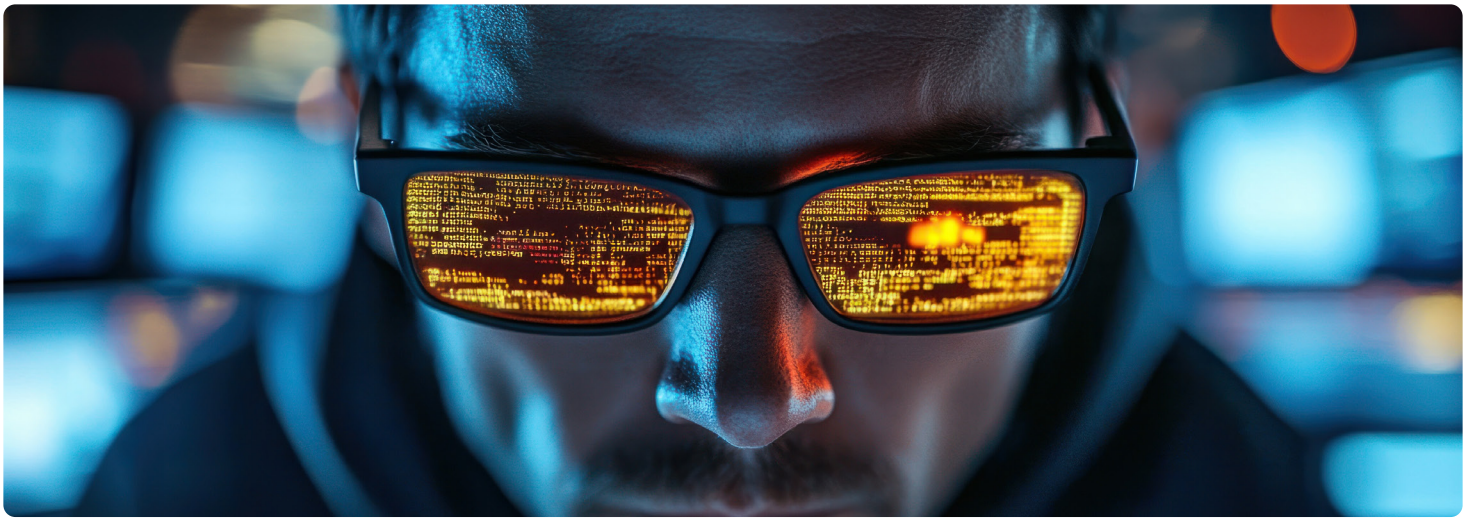
La certificación que valida las habilidades prácticas para planificar, ejecutar y reportar pruebas de penetración en redes, aplicaciones web, nube e IA.

¿Por qué debería asistir?

CompTIA PenTest+ certifica la capacidad de encontrar, atender y reportar vulnerabilidades en los sistemas. Cubre todas las fases de una prueba de penetración sobre superficies de ataque como la nube, las aplicaciones web, las API y el IoT, con foco en habilidades prácticas como la gestión de vulnerabilidades y el movimiento lateral. Está orientada a quienes buscan roles de pentester o de consultoría en seguridad.

Durante el curso, los participantes aprenden a planificar y delimitar el alcance de una prueba cumpliendo las obligaciones legales y éticas; a realizar reconocimiento activo y pasivo y a enumerar sistemas; a ejecutar escaneos de vulnerabilidades e interpretar y validar sus resultados; a llevar a cabo ataques de red, de autenticación, a hosts, a aplicaciones web, a la nube y a sistemas de IA con las herramientas adecuadas, y a mantener la persistencia, moverse lateralmente y documentar los hallazgos con recomendaciones de remediación. El programa cubre el 100 % de los objetivos del examen PT0-003.

5 días	5	26	Prácticos	Intermedio
DURACIÓN	DOMINIOS OFICIALES	OBJETIVOS	LABORATORIOS	NIVEL



¿Quién debería participar?

Pentesters y analistas de vulnerabilidades
Profesionales que evalúan la seguridad de redes, aplicaciones y nube mediante pruebas controladas.

Consultores de seguridad
Especialistas que realizan evaluaciones para clientes y presentan hallazgos y recomendaciones.

Equipos red team y de seguridad ofensiva
Integrantes de equipos que simulan ataques para medir la capacidad de detección y respuesta.

Profesionales con Security+ o CySA+
Analistas y administradores de seguridad que quieren sumar habilidades ofensivas a su perfil.

Objetivos de aprendizaje

- Planificar y delimitar pruebas de penetración cumpliendo las obligaciones legales y éticas.
- Redactar informes con hallazgos, análisis de riesgo y recomendaciones de remediación.
- Realizar reconocimiento activo y pasivo, recopilar información y enumerar sistemas.
- Modificar scripts en Python, PowerShell y Bash para automatizar el reconocimiento y los ataques.
- Ejecutar escaneos de vulnerabilidades, interpretar sus resultados y validar los hallazgos.
- Realizar ataques de red, de autenticación, a hosts, a aplicaciones web y a entornos en la nube.
- Comprender ataques a sistemas especializados y a la inteligencia artificial, como la inyección de prompts.
- Mantener la persistencia, moverse lateralmente y documentar las actividades de post-explotación.

Áreas de habilidad

Planificación y alcance | Aspectos legales y éticos | OSINT | Enumeración | Escaneo de vulnerabilidades | Ataques de red | Aplicaciones web | Ataques a la nube | Ataques a la IA | Ingeniería social | Movimiento lateral | Informes de pentest

Programa del curso

Duración: 5 días

Modalidades de formación

- **Presencial** — En aula, con instructor
- **Online** — En vivo, con instructor
- **Híbrida** — Aula y online combinadas

Módulo	Contenido
Dominio 1 Día 1	**1.0 Gestión del compromiso (13 %)** Actividades previas al compromiso y reglas de enfrentamiento; colaboración y comunicación; marcos y metodologías de pruebas; componentes del informe de pentest; análisis de hallazgos y recomendaciones de remediación.
Dominio 2 Día 2	**2.0 Reconocimiento y enumeración (21 %)** Técnicas de recopilación de información (OSINT, sniffing, escaneo de protocolos); técnicas de enumeración; modificación de scripts para reconocimiento; herramientas como Nmap, Wireshark y Shodan.
Dominio 3 Día 3	**3.0 Descubrimiento y análisis de vulnerabilidades (17 %)** Escaneos autenticados y no autenticados, SAST y DAST; análisis de resultados y falsos positivos; herramientas como Nessus, Nikto y OpenVAS; conceptos de seguridad física.
Dominio 4 Día 4	**4.0 Ataques y exploits (35 %)** Priorización de ataques; ataques de red, de autenticación, a hosts, a aplicaciones web, a la nube, inalámbricos y de ingeniería social; ataques a sistemas especializados y a la IA; uso de scripts para automatizar ataques.
Dominio 5 Día 5	**5.0 Post-explotación y movimiento lateral (14 %)** Persistencia; movimiento lateral; preparación y exfiltración de datos; limpieza y restauración del entorno. ✔ **Repaso integral y preparación para el examen** Repaso por dominio, práctica con preguntas basadas en desempeño (PBQ) y simulacro cronometrado del examen PT0-003.

El contenido sigue los 5 dominios y 26 objetivos oficiales del examen CompTIA PenTest+ PT0-003 (V3); el porcentaje indica el peso de cada dominio en el examen.

Examen y certificación

Título	CompTIA PenTest+ – Versión 3
Código	PT0-003
Preguntas	Máximo 90
Formato	Opción múltiple y preguntas basadas en desempeño
Duración	165 minutos
Aprobación	750 (escala de 100–900)
Idioma	Inglés, francés, japonés y portugués
Plataforma	Pearson VUE (centro de pruebas o en línea con OnVUE)

Requisitos de elegibilidad

- No hay requisitos obligatorios. CompTIA recomienda de 3 a 4 años de experiencia práctica como pentester y conocimientos equivalentes a Network+ y Security+.
- La versión anterior (PT0-002) se retiró el 17 de junio de 2025; la versión vigente es la V3 (PT0-003).

Ruta profesional CompTIA

PenTest+ es la certificación de seguridad ofensiva de nivel intermedio de la ruta de ciberseguridad de CompTIA: se apoya en Network+ y Security+, complementa a CySA+ en el lado defensivo y prepara el camino hacia SecurityX, el nivel experto.



Información general

- Material oficial de CompTIA, con laboratorios prácticos y preguntas de práctica.
- Instructor certificado y Savant Consultores como CompTIA Authorized Partner.
- Certificación acreditada por ANAB bajo la norma ISO/IEC 17024.
- Vigencia de 3 años, renovable mediante el programa de Educación Continua (CE) de CompTIA.

CompTIA Authorized Partner | ACADEMIC PARTNER

CompTIA PenTest+ CERTIFICATION Plus Series