CompTIA Pentest+

Visión General

El CompTIA PenTest+ es el único examen de prueba de penetración realizado en un centro de pruebas Pearson VUE con preguntas prácticas y de opción múltiple que se basan en el rendimiento para garantizar que cada candidato posee las habilidades, el conocimiento y la capacidad para realizar las tareas en los sistemas. El examen PenTest+ también incluye las habilidades de gestión para planificar, determinar y gestionar debilidades, no solo explotarlas.

PenTest+ es único debido a que nuestra certificación exige que el candidato demuestre capacidades y conocimiento prácticos para probar dispositivos en nuestros entornos tales como la nube y entornos móviles, además de los entornos tradicionales como el ordenador y los servidores.

Diferentes a otras certificaciones que tratan un contenido parecido, el énfasis de esta radica en los muchos aspectos de procedimientos y metodología que aporta que no son tratados por los demás contenidos de un alcance similar.

CompTIA PenTest+ valida su capacidad para identificar, mitigar y reportar vulnerabilidades del sistema. Abarca todas las etapas de las pruebas de penetración en superficies de ataque como la nube, aplicaciones web, API e IoT, y se centra en habilidades prácticas como la gestión de vulnerabilidades y el movimiento lateral. Esta certificación le proporciona la experiencia necesaria para progresar en su carrera como evaluador de penetración o consultor de seguridad.

.

¿Quien debería asistir?

- **Encargado de pruebas de penetración**
- **Encargado de pruebas de vulnerabilidades**
- **Analista de seguridad (II)**
- **Analista de evaluación de vulnerabilidades**
- **Operaciones de seguridad en redes**
- **Seguridad en vulnerabilidades en aplicaciones**

Agenda del curso

Duración: 5 días /40 horas

Día 1
- Pruebas de penetración: antes de comenzar
- Aplicación de actividades previas al compromiso

Día 2
- Enumeración y reconocimiento
- Escaneo e identificación de vulnerabilidades

Día 3
- Realización de ataques de pentest
- Ataques basados en la web

Día 4
- Ataques empresariales
- Ataques especializados

Día 5
- Realización de tareas de pruebas de penetración
- Informes y recomendaciones

Resumen de los objetivos del examen PenTest+ (V3)

Gestión del compromiso (13%)

- Planificación y alcance: definición de reglas de participación, ventanas de prueba y selección de objetivos.
- Cumplimiento legal y ético: garantizar cartas de autorización, informes obligatorios y cumplimiento de las regulaciones.
- Colaboración y comunicación: alineación con las partes interesadas a través de revisiones de pares, rutas de escalamiento y articulación de riesgos.
- Informes de pruebas de penetración: creación de informes con resúmenes ejecutivos, hallazgos y recomendaciones de remediación.

Reconocimiento y enumeración (21%)

- Reconocimiento activo y pasivo: recopilación de información mediante inteligencia de fuentes abiertas (OSINT), rastreo de redes y escaneo de protocolos.
- Técnicas de enumeración: realización de enumeración de DNS, descubrimiento de servicios y enumeración de directorios.
- Herramientas de reconocimiento: uso de herramientas como Nmap, Wireshark y Shodan para la recopilación de información.
- Modificación de scripts: personalización de scripts de Python, PowerShell y Bash para reconocimiento y enumeración.

Descubrimiento y análisis de vulnerabilidades (17%)

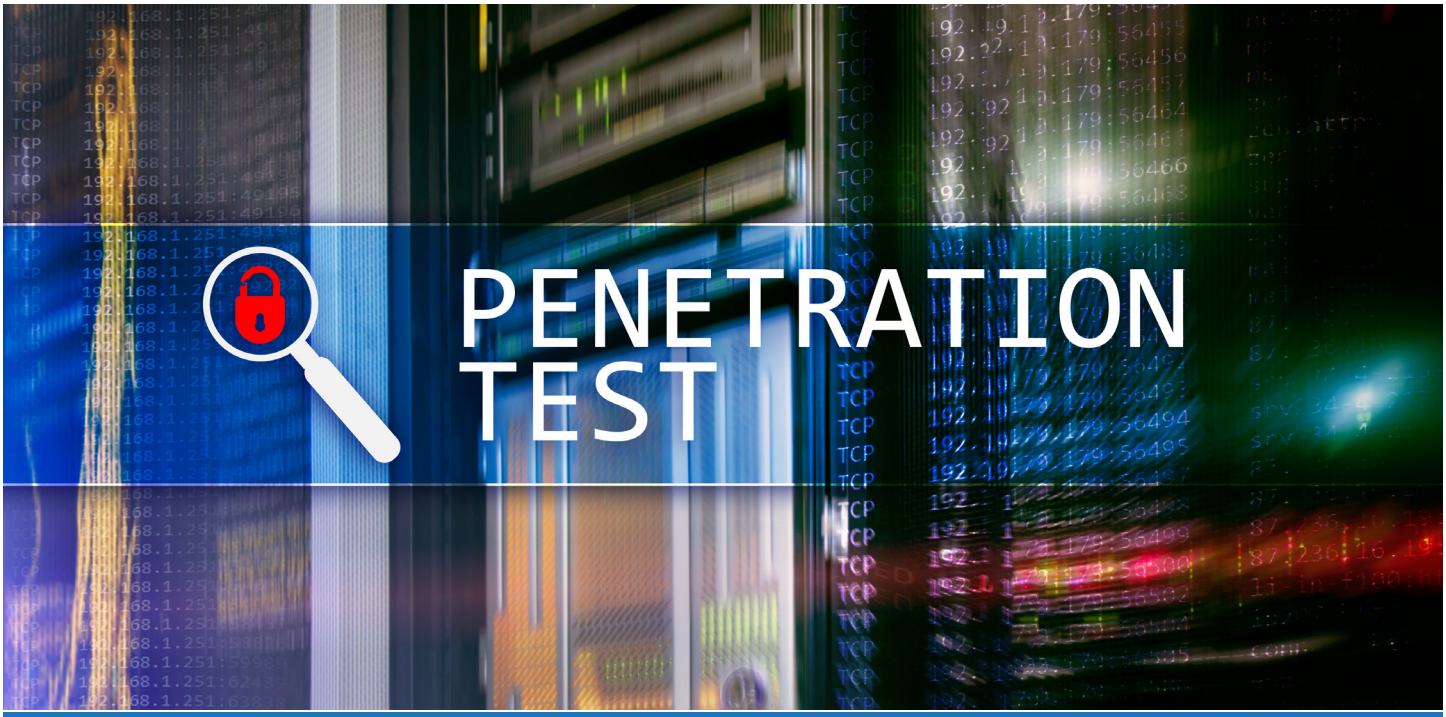
- Análisis de vulnerabilidades: realización de pruebas de seguridad de aplicaciones estáticas (SAST) autenticadas y no autenticadas y pruebas de seguridad de aplicaciones dinámicas (DAST).
- Análisis de resultados: validación de hallazgos, resolución de problemas de configuración e identificación de falsos positivos.
- Herramientas de descubrimiento: uso de herramientas como Nessus, Nikto y OpenVAS para el descubrimiento de vulnerabilidades.

Ataques y exploits (35%)

- Ataques de red: realización de saltos de VLAN, ataques en ruta y explotación de servicios.
- Ataques de autenticación: ejecución de ataques de fuerza bruta, pass-the-hash y robo de credenciales.
- Ataques basados en el host: realización de escalada de privilegios, inyección de procesos y volcado de credenciales.
- Ataques a aplicaciones web: ejecución de inyecciones SQL, secuencias de comandos entre sitios (XSS) y recorrido de directorios.
- Ataques basados en la nube: explotación de fugas de contenedores, ataques al servicio de metadatos y configuraciones incorrectas de gestión de identidad y acceso (IAM).
- Ataques de IA: explicación de la inyección rápida y la manipulación de modelos contra sistemas de inteligencia artificial.

Post-explotación y movimiento lateral (14%)

- Actividades posteriores a la explotación: establecer persistencia, realizar movimiento lateral y limpieza de artefactos.
- Documentación: creación de narrativas de ataques y provisión de recomendaciones de remediación.



Examen

Nombre del examen: PT0-003
Cantidad de preguntas: 90
Formato: Selección múltiple interactiva y desempeño
Disponibilidad: Pearson / VUE
Puntuación para pasar: 750l
Duración del examen: 165 minutos

Certificación

Después de completar con éxito el examen, recibirá el certificado digital de CompTIA que le acredita como un profesional certificado

Información general

- Único Centro de Entrenamiento Autorizado en el país
- Los honorarios del curso incluye el costo del examen
- Cada estudiante tendrá acceso a un entorno personalizado de aprendizaje con todos los contenidos necesarios para el curso
- Se incluye el acceso a los laboratorios virtuales para la realización de los ejercicios y aumentar así la comprensión y dominio de los objetivos del curso
- Como material para la preparación cada estudiante tendrá acceso a su propio entorno de preguntas de práctica para simular un ambiente de examen y mejorar las posibilidades de éxito
- Precio sugerido, USD 2,000 o su equivalente en pesos dominicanos

CompTIA Authorized Partner DELIVERY PARTNER

CompTIA PenTest+ CERTIFICATION Plus Series

SAVANT CONSULTORES

CompTIA