CompTIA PenTest+

Código: COM-117

Propuesta de Valor: COMPTIA

Duración: 40 Horas Académicas

La certificación CompTIA PenTest+ valida sus habilidades y conocimientos relacionados con las pruebas de penetración de segunda generación, la evaluación de vulnerabilidades y la gestión de vulnerabilidades en una variedad de sistemas y dispositivos, lo que la convierte en la última calificación en un mundo cada vez más móvil.

El examen PenTest+ también incluye las habilidades de gestión utilizadas para planificar, determinar y gestionar las debilidades, no solo explotarlas. PenTest+ es único porque nuestra certificación requiere un candidato para demostrar la habilidad práctica y el conocimiento para probar dispositivos en nuevos entornos como la nube y los dispositivos móviles, además de los escritorios y servidores tradicionales.

AUDIENCIA

- Este curso está diseñado para profesionales de TI que desean desarrollar habilidades de prueba de penetración para permitirles identificar vulnerabilidades en el sistema de información y técnicas de remediación eficaces para esas vulnerabilidades.
- Los estudiantes seleccionados que también necesitan ofrecer recomendaciones prácticas para la acción para proteger adecuadamente los sistemas de información y sus contenidos derivarán esas habilidades de este curso.

PRE REQUISITOS

- No tiene prerrequisitos previos.

OBJETIVOS

- Pruebas de penetración plan y alcance.
- Realizar reconocimiento pasivo.
- Realizar pruebas no técnicas para recopilar información.
- Reconocimiento activo conductivo.
- Analizar vulnerabilidades.
- Penetrar en las redes.
- Explotar vulnerabilidades basadas en host.
- Aplicaciones de prueba y completar tareas post-exploit.

- Analizar e informar resultados de la prueba de la pluma.

CERTIFICACIÓN DISPONIBLE

- El curso lo prepara para la certificación: **CompTIA PenTest+** PT0-001.

CONTENIDO

1. PLANIFICACIÓN Y DETERMINACIÓN DEL ALCANCE DE LAS PRUEBAS DE PENETRACIÓN

1.1. INTRODUCCIÓN A LOS CONCEPTOS DE PRUEBAS DE PENETRACIÓN
1.2. PLANIFIQUE UNA PARTICIPACIÓN EN LA PRUEBA DE LÁPIZ
1.3. ALCANCE Y NEGOCIACIÓN DE UN COMPROMISO DE PRUEBA DE PENETRACIÓN
1.4. PREPÁRESE PARA UN COMPROMISO DE PRUEBA DE PLUMA

2. REALIZACIÓN DE RECONOCIMIENTO PASIVO

2.1. RECOPILAR INFORMACIÓN DE ANTECEDENTES
2.2. PREPARAR LOS ANTECEDENTES PARA LOS PRÓXIMOS PASOS

3. REALIZACIÓN DE PRUEBAS NO TÉCNICAS

3.1. REALIZAR PRUEBAS DE INGENIERÍA SOCIAL
3.2. REALIZAR PRUEBAS DE SEGURIDAD FÍSICA EN LAS INSTALACIONES

4. REALIZACIÓN DE RECONOCIMIENTO ACTIVO

4.1. ESCANEAR REDES
4.2. ENUMERAR DESTINOS
4.3. ANÁLISIS DE VULNERABILIDADES
4.4. ANALIZAR GUIONES BÁSICOS

5. ANÁLISIS DE VULNERABILIDADES

5.1. ANALIZAR LOS RESULTADOS DEL ANÁLISIS DE VULNERABILIDADES
5.2. APROVECHAR LA INFORMACIÓN PARA PREPARARSE PARA LA EXPLOTACIÓN

6. PENETRAR REDES

6.1. EXPLOTAR LAS VULNERABILIDADES BASADAS EN LA RED
6.2. EXPLOTE LAS VULNERABILIDADES INALÁMBRICAS Y BASADAS EN RF
6.3. EXPLOTAR SISTEMAS ESPECIALIZADOS

7. EXPLOTACIÓN DE VULNERABILIDADES BASADAS EN HOST

7.1. EXPLOTAR VULNERABILIDADES BASADAS EN WINDOWS
7.2. EXPLOIT * VULNERABILIDADES BASADAS EN NIX

8. PRUEBA DE APLICACIONES

8.1. EXPLOTAR LAS VULNERABILIDADES DE LAS APLICACIONES WEB
8.2. PROBAR EL CÓDIGO FUENTE Y LAS APLICACIONES COMPILADAS

9. COMPLETAR TAREAS POSTERIORES A LA EXPLOTACIÓN

9.1. UTILICE TÉCNICAS DE MOVIMIENTO LATERAL
9.2. UTILICE TÉCNICAS DE PERSISTENCIA
9.3. UTILICE TÉCNICAS ANTI-FORENSES

10. ANÁLISIS E INFORMES DE LOS RESULTADOS DE LA PRUEBA DE LÁPIZ

10.1. ANALIZAR LOS DATOS DE LA PRUEBA DE LA PLUMA
10.2. DESARROLLAR RECOMENDACIONES PARA ESTRATEGIAS DE MITIGACIÓN
10.3. REDACCIÓN Y GESTIÓN DE INFORMES
10.4. REALIZACIÓN DE ACTIVIDADES POSTERIORES A LA ENTREGA DEL INFORME

BENEFICIOS

- Después de completar este curso, podrá planificar, realizar, analizar e informar sobre las pruebas de penetración.