CompTIA PenTest+

Código: COM-117

Propuesta de Valor: COMPTIA

Duración: 40 Horas

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+ PT0-002**.

CONTENIDO

1. ALCANCE DE LOS REQUISITOS ORGANIZACIONALES/DEL CLIENTE

1.1. DEFINIR PETESTING ORGANIZACIONAL
1.2. RECONOCIMIENTO DE REQUISITOS DE CUMPLIMIENTO
1.3. COMPARAR ESTÁNDARES Y METODOLOGÍAS
1.4. DESCRIBIR FORMAS DE MANTENER EL PROFESIONALISMO

2. DEFINICIÓN DE LAS REGLAS DE COMPROMISO

2.1. EVALUAR LAS CONSIDERACIONES AMBIENTALES
2.2. RESUMEN DE LAS REGLAS DE ENFRENTAMIENTO
2.3. PREPARAR DOCUMENTOS LEGALES

3. FOOTPRINTING Y RECOPILACIÓN DE INTELIGENCIA

3.1. DESCUBRA EL OBJETIVO
3.2. REUNIR DATOS ESENCIALES
3.3. COMPILAR INFORMACIÓN DEL SITIO WEB
3.4. DESCUBRA HERRAMIENTAS DE INTELIGENCIA DE CÓDIGO ABIERTO

4. EVALUACIÓN DE VULNERABILIDADES HUMANAS Y FÍSICAS

4.1. EXPLOTAR LA PSIQUE HUMANA
4.2. RESUMIR LOS ATAQUES FÍSICOS
4.3. USAR HERRAMIENTAS PARA LANZAR UN ATAQUE DE INGENIERÍA SOCIAL

5. PREPARACIÓN DEL ANÁLISIS DE VULNERABILIDADES

5.1. PLANIFICAR LA EXPLORACIÓN DE VULNERABILIDADES
5.2. DETECTAR DEFENSAS
5.3. UTILIZAR HERRAMIENTAS DE ESCANEO

6. ANÁLISIS DE VULNERABILIDADES LÓGICAS

6.1. ANALIZAR OBJETIVOS IDENTIFICADOS
6.2. EVALUAR EL TRÁFICO DE RED
6.3. DESCUBRIR ACTIVOS INALÁMBRICOS

7. ANÁLISIS DE RESULTADOS DE ESCANEO

7.1. DESCUBRA NMAP Y NSE
7.2. ENUMERAR HOSTS DE RED
7.3. ANALIZAR LA SALIDA DE LOS ESCANEOS

8. EVITAR LA DETECCIÓN Y CUBRIR LAS HUELLAS

8.1. DETECCIÓN DE EVASIÓN
8.2. UTILICE LA ESTEGANOGRAFÍA PARA OCULTAR Y OCULTAR
8.3. ESTABLECER UN CANAL ENCUBIERTO

9. EXPLOTACIÓN DE LA LAN Y LA NUBE

9.1. ENUMERACIÓN DE HOSTS
9.2. PROTOCOLOS LAN DE ATAQUE
9.3. COMPARAR HERRAMIENTAS DE EXPLOTACIÓN
9.4. DESCUBRA LAS VULNERABILIDADES DE LA NUBE
9.5. EXPLORE LOS ATAQUES BASADOS EN LA NUBE

10. PRUEBA DE REDES INALÁMBRICAS

10.1. DESCUBRIR ATAQUES INALÁMBRICOS
10.2. EXPLORAR HERRAMIENTAS INALÁMBRICAS

11. ORIENTACIÓN A DISPOSITIVOS MÓVILES

11.1. RECONOCER LAS VULNERABILIDADES DE LOS DISPOSITIVOS MÓVILES
11.2. LANZAR ATAQUES EN DISPOSITIVOS MÓVILES
11.3. RESUMEN DE HERRAMIENTAS DE EVALUACIÓN PARA DISPOSITIVOS MÓVILES

12. ATACAR SISTEMAS ESPECIALIZADOS

12.1. IDENTIFICAR ATAQUES EN EL IOT
12.2. RECONOCER OTROS SISTEMAS VULNERABLES
12.3. EXPLICAR LAS VULNERABILIDADES DE LAS MÁQUINAS VIRTUALES

13. ATAQUES BASADOS EN APLICACIONES WEB

13.1. RECONOCER VULNERABILIDADES WEB
13.2. ATAQUES DE SESIÓN DE LANZAMIENTO
13.3. ATAQUES DE INYECCIÓN DE PLANES
13.4. IDENTIFICAR HERRAMIENTAS

14. REALIZAR PIRATERÍA DEL SISTEMA

14.1. HACKEO DE SISTEMAS
14.2. USAR HERRAMIENTAS DE ACCESO REMOTO
14.3. ANALIZAR CÓDIGO DE EXPLOTACIÓN

15. SCRIPTING Y DESARROLLO DE SOFTWARE

15.1. ANÁLISIS DE SECUENCIAS DE COMANDOS Y MUESTRAS DE CÓDIGO
15.2. CREAR CONSTRUCCIONES LÓGICAS
15.3. AUTOMATIZACIÓN DE PRUEBAS DE PENETRACIÓN

16. APROVECHANDO EL ATAQUE: PIVOTAR Y PENETRAR

16.1. CREDENCIALES DE PRUEBA
16.2. MOVERSE POR TODO EL SISTEMA
16.3. MANTENER LA PERSISTENCIA

17. COMUNICACIÓN DURANTE LA PRUEBA DE PENETRACIÓN PROCESO

17.1. DEFINIR LA RUTA DE COMUNICACIÓN
17.2. DISPARADORES DE COMUNICACIÓN
17.3. USAR HERRAMIENTAS INTEGRADAS PARA GENERAR INFORMES

18. RESUMEN DE LOS COMPONENTES DEL INFORME

18.1. IDENTIFICAR LA AUDIENCIA DEL INFORME
18.2. CONTENIDO DE LA LISTA DEL INFORME
18.3. DEFINIR MEJORES PRÁCTICAS PARA INFORMES

19. RECOMENDACIÓN DE REMEDIACIÓN

19.1. EMPLEAR CONTROLES TÉCNICOS
19.2. CONTROLES ADMINISTRATIVOS Y OPERATIVOS
19.3. CONTROLES FÍSICOS

20. REALIZACIÓN DE ACTIVIDADES POSTERIORES A LA ENTREGA DE INFORMES

20.1. LIMPIEZA POSTERIOR AL COMPROMISO
20.2. ACCIONES DE SEGUIMIENTO

BENEFICIOS

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