CompTIA

Pentest+

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.

Objetivos del curso

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 solución.

Reconocimiento y enumeración (21%)

- **Reconocimiento activo y pasivo:** recopilación de información utilizando inteligencia de fuente abierta (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.

Postexplotación 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.

Habilidades aprendidas

- Planificar y delimitar pruebas de penetración garantizando al mismo tiempo el cumplimiento de los requisitos legales y éticos, y desarrollar informes detallados con recomendaciones de remediación para respaldar la gestión del compromiso.
- Realizar reconocimiento activo y pasivo, recopilar información y enumerar sistemas para descubrir vulnerabilidades de manera efectiva.
- Realizar análisis de vulnerabilidad, analizar resultados y validar hallazgos para identificar y abordar debilidades de seguridad.
- Ejecute ataques a redes, host, aplicaciones web y en la nube utilizando herramientas y técnicas adecuadas para probar las defensas del sistema.
- Mantener la persistencia, realizar movimientos laterales y documentar los hallazgos para respaldar los esfuerzos de remediación durante las actividades posteriores a la explotación.