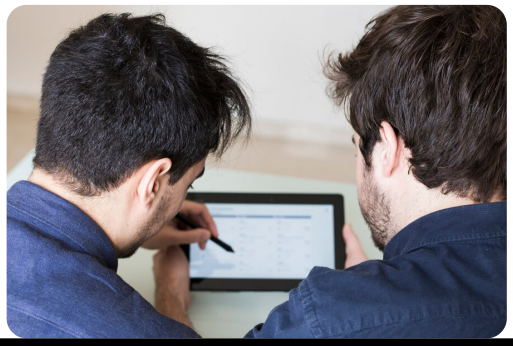

IFCT125. Test de intrusión

Sku: IFCT125_EC

Horas: 60

OBJETIVOS

Manejar tanto los procedimientos como las herramientas y técnicas para atacar los sistemasinformáticos, identificando si las aplicaciones tienen alguna vulnerabilidad y si ésta es explotableen las condiciones del entorno de trabajo, con las medidas de protección disponibles.

CONTENIDOS

1. TEST DE INTRUSIÓN Y TIPOLOGÍA DE HERRAMIENTAS
1.1 Distinción entre test de intrusión y auditoría
1.1.1. Objetivos
1.1.2. Elementos diferenciadores
1.2 Clasificación de la tipología según la información que dispongamos
1.2.1. Caja blanca
1.2.2. Caja negra
1.2.3. Caja gris
1.3 Clasificación de la tipología en función de los servicios a testear:
1.3.1. Pen test de red
1.3.2. Pen test de redes inalámbricas
1.3.3. Pen test de sistemas
1.3.4. Pen test de aplicaciones web
1.3.5. Pen test de ingeniería social

2. METODOLOGÍAS DE TEST DE INTRUSIÓN
2.1 Descripción de las fases de un test de intrusión
2.1.1. Planificación del test
2.1.2. Análisis del test
2.1.3. Informes con los resultados del test
2.2 Definición de Conceptos
2.2.1. Alcance del test
2.2.2. Vector de ataque
2.3 Clasificación OSSTMM (Open Source Security Testing Methodology Manual)

2.3.1. Seguridad física
2.3.2. Seguridad de los procesos
2.3.3. Seguridad en las tecnologías de Internet
2.3.4. Seguridad en las comunicaciones
2.3.5. Seguridad inalámbrica
2.3.6. Seguridad de la información
2.3.7. RAV (Risk assessment value)
2.4 Clasificación OWASP (Open Web Applications Security Project)
2.4.1. Pruebas de gestión de la configuración y la implementación
2.4.2. Pruebas de gestión de identidad
2.4.3. Prueba de autenticación
2.4.4. Prueba de autorización
2.4.5. Prueba de gestión de sesiones
2.4.6. Prueba de validación de entrada
2.4.7. Prueba de manejo de errores
2.4.8. Prueba de criptografía débil
2.4.9. Pruebas de lógica empresarial
2.4.10. Pruebas del lado del cliente
2.4.11. Pruebas de API
2.5 Diferenciación entre OSSTMM y OWASP

3. HERRAMIENTAS PARA LA EJECUCIÓN DE TEST DE INTRUSIÓN
3.1 Clasificación de herramientas genéricas
3.1.1. Burp Suite
3.1.2. OpenVas
3.1.3. Nessus
3.1.4. Metasploit
3.1.5. Kali Linux
3.2 Clasificación de herramientas de red
3.2.1. Nmap
3.2.2. Aircrack-ng
3.2.3. Wireshark
3.2.4. Zmap
3.2.5. Ettercap
3.3 Clasificación de herramientas de robo de contraseñas
3.3.1. Hydra
3.3.2. John de Ripper
3.3.3. Hashcat

4. RESULTADOS E INFORMES
4.1 Descripción de herramientas de ayuda a la documentación
4.1.1. Dradis
4.1.2. Faraday
4.2 Elaboración de informes
4.2.1. Evaluación y análisis de los resultados

4.2.2. Especificación de test realizados
4.2.3. Resultados técnicos
4.2.4. Recomendaciones
4.3 Definición de políticas de conservación de los registros:
4.3.1. Granularidad y perdurabilidad de los datos registrados en función de fuentes y relevancia
4.3.2. Requerimientos normativos y contractuales

5. PLANIFICACIÓN Y EJECUCIÓN DE UN TEST DE INTRUSIÓN
5.1 Selección de la metodología más adecuada para realizar un test de intrusión.
5.1.1. Definir el alcance
5.1.2. Determinar vectores de ataque
5.1.3. Planificación para llevarla a cabo.
5.2 Selección del tipo de test de intrusión para determinar la explotabilidad de las vulnerabilidades.
5.2.1. Determinar el test en función del alcance
5.2.2. Ejecución del test seleccionado
5.2.3. Obtención de resultados
5.3 Elaboración del informe de test de intrusión.
5.3.1. Recopilación y ordenación de la información
5.3.2. Redacción del informe