Reconnaissance

Passive Reconnaissance: Obtener información sin interactuar directamente con el sistema.

- Búsqueda de información pública a través de motores de búsqueda (Google, Shodan, etc.)
- Enumeración de subdominios para identificar posibles puntos de entrada adicionales.
- Recopilación de información del dominio y direcciones IP.

Active Reconnaissance: Interactuar directamente con el sistema objetivo para obtener información más detallada y específica:

- Identificación de versiones de servicios y aplicaciones en ejecución
- Identificación de las tecnologías y frameworks utilizados por la aplicación web (e.g., servidores web, bases de datos, lenguajes de programación, etc.).
- Enumeración de directorios y archivos accesibles públicamente.
- Entender cómo funciona la aplicación, funcionalidades , etc

Scanning/Analisis de Vulnerabilidades

Escaneo de vulnerabilidades mediante herramientas automatizadas
Escaneo de puertos en busca de servicios y configuraciones vulnerables

Exploitation

- Explotación de vulnerabilidades conocidas (CVE) y previamente encontradas
- Búsqueda de vulnerabilidades de manera manual : Access control,Business logic,Authentication,Race conditions,Api testing etc

Post-Exploitation

- Extracción de información “valiosa”
- Instalación de puertas traseras o shells web.
- Creación de usuarios ocultos o modificación de configuraciones para mantener acceso.
- Acceder a otros sistemas o servicios accesibles desde el sistema comprometido
- Eliminación de registros de logs,scripts que hayamos podido generar.

Reporting

Documentation:

Elaboración de un informe detallado con los resultados del pentesting.

- Descripción de las vulnerabilidades identificadas, incluyendo impacto y riesgo.
- Evidencias y pruebas de explotación realizadas.
- Recomendaciones para la mitigación de las vulnerabilidades encontradas.
- Resumen ejecutivo y técnico del estado de seguridad de la aplicación web.
- Propuesta de un plan de acción para la remediación de los problemas de seguridad identificados.