Algunas herramientas para reconocimiento de forma pasiva

1. **Shodan:**
    - Shodan es un motor de búsqueda que permite buscar dispositivos conectados a Internet, como cámaras, servidores, enrutadores, y más, proporcionando información detallada sobre estos dispositivos.
2. **Censys:**
    - Censys es otro motor de búsqueda que ayuda a descubrir dispositivos y servidores en Internet y proporciona información sobre sus servicios y certificados.
3. **theHarvester:**
    - theHarvester es una herramienta de código abierto que recopila información de fuentes públicas, como motores de búsqueda, para obtener direcciones de correo electrónico, subdominios, nombres de host, y más.
4. **Maltego:**
    - Maltego es una herramienta de minería de datos que permite recopilar información sobre personas, organizaciones, relaciones y redes en función de la información pública disponible en la web.
5. **SpiderFoot:**
    - SpiderFoot es una herramienta de fuente abierta que automatiza la recopilación de información sobre objetivos utilizando múltiples fuentes públicas, como redes sociales, motores de búsqueda, servicios DNS y más.
6. **Sublist3r:**
    - Sublist3r es una herramienta que ayuda a enumerar subdominios a partir de búsquedas en motores de búsqueda y sitios web públicos.
7. Dedigger
    - De Digger es un sitio web que le permite encontrar cualquier tipo de archivos que estén disponibles públicamente en Google Drive. 👀

8. **Fofa**
    - Es un motor de búsqueda y plataforma de análisis que se centra en descubrir y recopilar información pública disponible en línea. Fue desarrollado por la empresa chino-española Cyberspace y se ha convertido en una herramienta popular en el ámbito de la ciberseguridad y la inteligencia cibernética.
9. **Subfinder**
    - Es una herramienta de descubrimiento de subdominios que devuelve subdominios válidos para sitios web, utilizando fuentes pasivas en línea. Tiene una arquitectura modular simple y está optimizada para la velocidad. subfinder está diseñado para hacer una sola cosa: enumeración pasiva de subdominios, y lo hace muy bien.

Algunas herramientas para reconocimiento de forma activa

1. **Nmap:**
    - **Nmap (Network Mapper) es una herramienta de código abierto ampliamente utilizada para escanear puertos y realizar descubrimiento de hosts en una red, identificando servicios y sistemas operativos.**
2. **Zenmap:**
    - **Zenmap es la interfaz gráfica de usuario para Nmap y facilita la configuración y visualización de resultados de escaneos de red.**
3. **Masscan:**
    - **Masscan es una herramienta de escaneo de puertos de alta velocidad que puede escanear toda la internet en minutos, proporcionando una vista rápida de los servicios en una red.**
4. **Metasploit Framework:**
    - **Metasploit es un marco de desarrollo y ejecución de exploits que permite probar sistemas en busca de vulnerabilidades y realizar pruebas de penetración de manera controlada.**
5. **Burp Suite:**
    - **Burp Suite es una suite integral de herramientas para la realización de pruebas de seguridad en aplicaciones web, incluyendo escaneo de vulnerabilidades, intrusión y análisis de tráfico.**
6. **Acunetix:**
    - **Acunetix es una herramienta de escaneo de vulnerabilidades web que identifica y explora vulnerabilidades en aplicaciones web y sitios web.**
7. **Aircrack-ng:**
    - **Aircrack-ng es una suite de herramientas de seguridad inalámbrica que se utiliza para auditar y analizar la seguridad de redes inalámbricas.**
8. **THC-Hydra:**
    - **Hydra es una herramienta de fuerza bruta que permite probar credenciales en diferentes servicios, como FTP, SSH, HTTP, y más.**
9. **Sqlmap:**
    - **Sqlmap es una herramienta de prueba de penetración que automatiza la detección y explotación de vulnerabilidades de inyección de SQL en aplicaciones web.**

10. **Gobuster:**

    - **Gobuster es una herramienta de fuerza bruta que busca directorios y archivos en servidores web, útil para descubrir contenido oculto o no enlazado.**

11. **Wfuzz:**

    - **Wfuzz es una herramienta de evaluación de seguridad que permite realizar ataques de fuerza bruta para descubrir vulnerabilidades en aplicaciones web.**