La recolección de inteligencia activa es una fase crucial en la realización de pruebas de penetración y evaluación de la seguridad, donde se recopila información sobre el objetivo de manera directa e interactiva. A diferencia de la recolección pasiva, que se basa en la obtención de información sin interacción directa con el objetivo, la recolección activa implica interactuar directamente con los sistemas y redes objetivo. A continuación se presentan algunas técnicas y herramientas comunes utilizadas en la recolección de inteligencia activa:

**Técnicas de Recolección de Inteligencia Activa**

1. **Escaneo de Puertos**:
   * **Descripción**: Identificación de los puertos abiertos en un sistema objetivo.
   * **Herramientas**: Nmap, Masscan.
   * **Comando Nmap Ejemplo**:

bash

Copy code

nmap -sS -p 1-65535 -T4 <IP objetivo>

1. **Fingerprinting de Servicios**:
   * **Descripción**: Identificación de servicios y versiones de software que se ejecutan en los puertos abiertos.
   * **Herramientas**: Nmap, Netcat, amap.
   * **Comando Nmap Ejemplo**:

bash

Copy code

nmap -sV <IP objetivo>

1. **Escaneo de Vulnerabilidades**:
   * **Descripción**: Identificación de vulnerabilidades conocidas en los sistemas y servicios del objetivo.
   * **Herramientas**: OpenVAS, Nessus, Nikto.
   * **Comando Nikto Ejemplo**:

bash

Copy code

nikto -h <IP objetivo>

1. **Enumeración de Redes WiFi**:
   * **Descripción**: Identificación de redes inalámbricas disponibles y recopilación de información sobre ellas.
   * **Herramientas**: Aircrack-ng suite, Kismet.
   * **Comando Airodump-ng Ejemplo**:

bash

Copy code

airodump-ng <interfaz de red inalámbrica>

1. **Enumeración de Usuarios y Grupos**:
   * **Descripción**: Obtención de información sobre usuarios y grupos en un sistema o red.
   * **Herramientas**: enum4linux, Nmap scripts, rpcclient.
   * **Comando enum4linux Ejemplo**:

bash

Copy code

enum4linux -a <IP objetivo>

1. **Escaneo de Red Interna**:
   * **Descripción**: Escaneo de dispositivos y servicios en una red interna después de obtener acceso inicial.
   * **Herramientas**: Nmap, ARP scan, Netdiscover.
   * **Comando ARP-scan Ejemplo**:

bash

Copy code

arp-scan --interface=<interfaz de red> <rango de IP>

1. **Captura de Tráfico**:
   * **Descripción**: Monitoreo y análisis del tráfico de red para recopilar información sensible.
   * **Herramientas**: Wireshark, Tcpdump.
   * **Comando Tcpdump Ejemplo**:

bash

Copy code

tcpdump -i <interfaz de red> -w captura.pcap

1. **Fingerprinting de Sistemas Operativos**:
   * **Descripción**: Identificación del sistema operativo que se está ejecutando en un objetivo.
   * **Herramientas**: Nmap, xProbe2.
   * **Comando Nmap Ejemplo**:

bash

Copy code

nmap -O <IP objetivo>

**Herramientas Comunes para Recolección de Inteligencia Activa**

1. **Nmap**:
   * **Descripción**: Herramienta de escaneo de red y puertos ampliamente utilizada.
   * **Sitio web**: [Nmap](https://nmap.org)
2. **Wireshark**:
   * **Descripción**: Analizador de protocolos de red para la captura y análisis de tráfico.
   * **Sitio web**: [Wireshark](https://www.wireshark.org)
3. **Metasploit**:
   * **Descripción**: Plataforma para el desarrollo y ejecución de exploits.
   * **Sitio web**: [Metasploit](https://www.metasploit.com)
4. **OpenVAS**:
   * **Descripción**: Sistema de escaneo de vulnerabilidades y gestión.
   * **Sitio web**: [OpenVAS](https://www.openvas.org)
5. **Nikto**:
   * **Descripción**: Escáner de servidores web que prueba la presencia de vulnerabilidades.
   * **Sitio web**: Nikto
6. **Aircrack-ng**:
   * **Descripción**: Conjunto de herramientas para auditoría de redes WiFi.
   * **Sitio web**: [Aircrack-ng](https://www.aircrack-ng.org)

**Ejemplo de un Proceso de Recolección de Inteligencia Activa**

1. **Escaneo de Puertos**:
   * **Objetivo**: Identificar puertos abiertos.
   * **Comando**:

bash

Copy code

nmap -sS -T4 <IP objetivo>

1. **Fingerprinting de Servicios**:
   * **Objetivo**: Determinar los servicios y versiones que se ejecutan.
   * **Comando**:

bash

Copy code

nmap -sV <IP objetivo>

1. **Escaneo de Vulnerabilidades**:
   * **Objetivo**: Encontrar vulnerabilidades conocidas.
   * **Comando**:

bash

Copy code

openvas-start

1. **Enumeración de Usuarios y Grupos**:
   * **Objetivo**: Obtener información sobre usuarios y grupos.
   * **Comando**:

bash

Copy code

enum4linux -a <IP objetivo>

1. **Captura de Tráfico**:
   * **Objetivo**: Analizar el tráfico de red.
   * **Comando**:

bash

Copy code

tcpdump -i eth0 -w captura.pcap

**Consideraciones Éticas y Legales**

Es importante recordar que la recolección de inteligencia activa sin el permiso explícito del propietario del sistema o red es ilegal y puede tener graves consecuencias legales. Las pruebas de penetración y auditorías de seguridad deben realizarse siempre con el consentimiento adecuado y dentro del marco legal correspondiente.