**Técnicas relacionadas con “Information Gathering”**

La recolección de información es la capacidad de obtener la mayor cantidad de datos de un potencial blanco a auditar o atacar.

La misma se puede realizar tanto de manera externa al blanco como interna, es decir que podemos utilizar un número muy grande de herramientas disponibles para recolectar la mayor cantidad de información del equipo sin haber accedido a el y por otro lado contamos con herramientas que nos brinda el propio sistema a efectis de realizar la recolección.

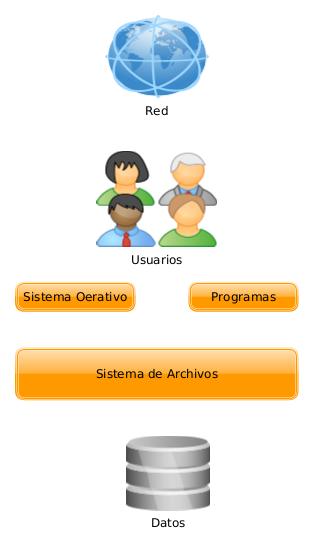
Hay que tener presente que cuando se ataca y explota un servicio determinado, este corre bajo el ID de un usuario puntual, con lo cual , cuantas más herramientas tengamos disponibles para utilizar, mayor recolección de información vamos a poder lograr.

Linux nos ofrece una cantidad de herramientas y utilidades ya instaladas por defecto, las cuales perfectamente pueden servirnos (y van a servirnos) para este proyecto.

Para poder tener claro la información que necesitamos recolectar, primero tenemos que tener claro que es lo que vamos a revisar, con lo cual vamos primero a separar en diferentes capas de acceso.

Tomando como base principal los datos a proteger (la cual sería la capa “interna”) a partir de ahí nos vamos alejando hasta la capa más “externa” que es la red.

Hecha la aclaración tenemos un diagrama que es el siguiente:



Descripción de las capas y herramientas disponibles en cada una de ella

**Red**: Puede variar de acuerdo a la red donde se encuentre el equipo. Lo importante es que aquí tenemos varias opciones a realizar a efectos de mejorar la misma.

Algunas herramientas disponibles son:

* netstat / ss: Ver conexiones activas, servicios en escucha, servicios por protocolo, estado de conexiones, procesos asociados, contextos, enrutamiento, etc
* route: Tabla de ruteo
* ip / ifconfig: información de las interfaces de red, estado, errores, dirección MAC, túneles, ruteo, etc
* arp: Tabla de direcciones MAC
* ethtool: Estado de las interfaces de red, driver asociado, estadísticas, configuraciones

**Usuarios**: Esta capa refiere a los permisos de acceso de los usuarios en el sistema e incluye autentificación, autorización y acceso.

Hay muchos controles aquí que implican verificaciones a nivel de permisos. Se mencionan algunos ejemplos:

* Usuarios con id 0
* Terminales habilitadas para realizar login
* Cuentas con o sin shell
* Grupos a los cuales pertenece un usuario
* Restricciones mediante PAM (fortalecimiento de contraseñas, forzar cambios, historial, etc)

**Sistema Operativo**: En este punto, hacemos referencia a todo lo que implica el sistema operativo auditado o comprometido. Esto incluye procesos en ejecución, servicios por defecto habilitados, aplicaciones y su configuración, manejo de dispositivos, etc.

Ejemplos de control:

* Logs de auditoría registrados y guardados en sistema centralizado
* Revisión de violaciones de acceso
* Permisos de ejecución de herramientas sensibles (o peligrosas)
* Control de accesos a comandos como root (su)
* Dispositivos y herramientas del sistema protegidos contra usuarios no autorizados (sniffers, analizadores de protocolo, herramientas de red, etc)

**Sistema de Archivos**: Es importante restringir los permisos de acceso de los usuarios a determinados lugares del sistema de archivos que no deben acceder. Ejemplos:

* Registros de sucesos
* Archivos y directorios sin propietario
* Permisos de acceso a archivos de configuración
* Minimizar los directorios del sistema operativo con permisos totales

**Datos**: Esta es la información que estamos protegiendo. Debemos tener claro que protegemos y como lo estamos haciendo, Ejemplos:

* Si es una base de datos, permisos de archivos, usuarios, contraseñas, accesos anónimos, bases de test habilitadas
* Archivos de texto, permisos mencionados anteriormente