FUNDAMENTOS DE SEGURIDAD INFORMÁTICA Nivel 2

RECOPILACIÓN DE LA INFORMACIÓN

Capacítate para el empleo | FUNDACIÓN Carlos Slim

La recopilación de información o *footpring* es el proceso de recolección de datos para un objetivo, el cual ocupan los *hackers* en sus etapas iniciales para desarrollar su actividad.

Tipos de recolección

De fuente abierta

Es el más seguro conforme a la ley, ya que **los *hackers* recolectan información sin recibir alguna sanción.** Por ejemplo, la identificación de cuentas de dirección de correo electrónico y su número telefónico.

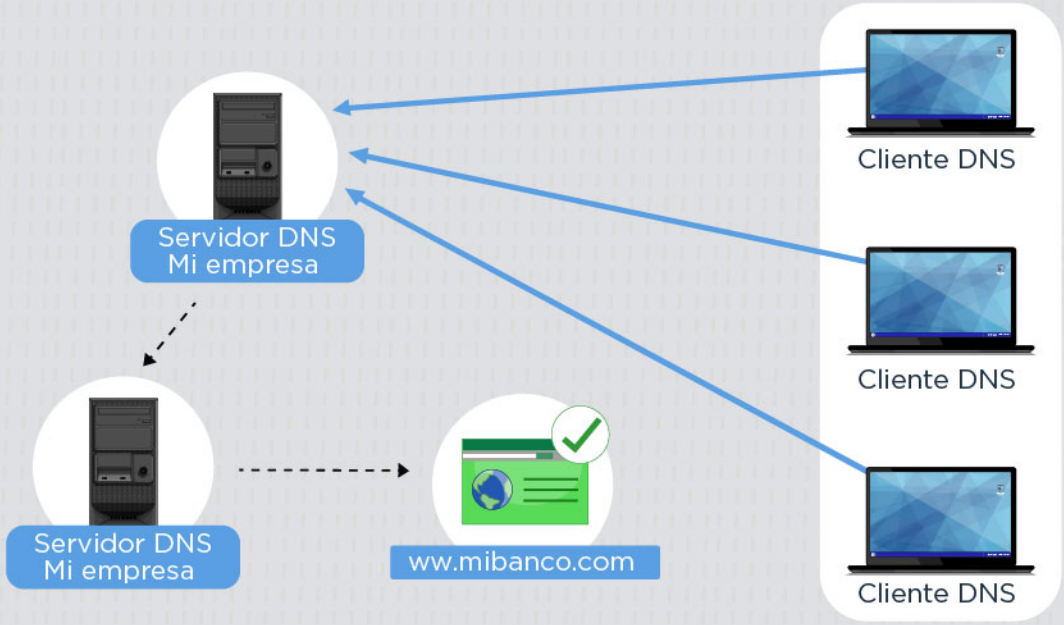
Basados en red

En esta categoría **los *hacktivistas* pueden recuperar información de un nombre de usuario,** datos que son compartidos entre individuos y servicios de red.

RECOPILACIÓN DE LA INFORMACIÓN

Interrogación del sistema de nombres de dominio o DNS

Es la **solicitud que se hace al servidor DNS para obtener nombres de los equipos de usuarios** y direcciones de red para potenciales sistemas objetivos.



Técnicas

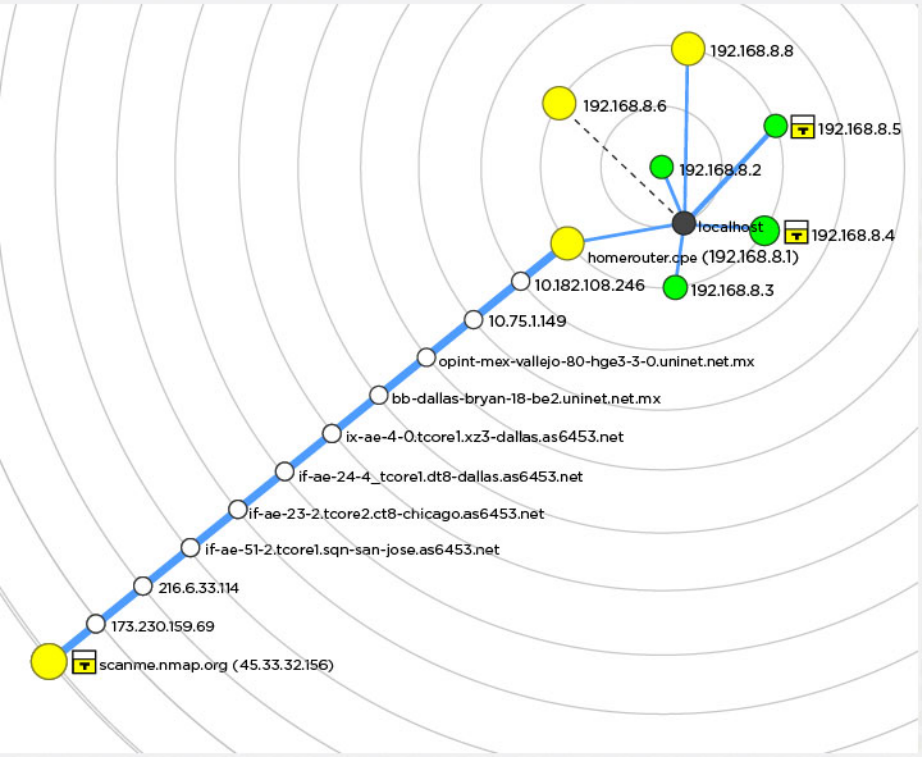
Para poder recabar la información, los ***hackers*** **usan las siguientes técnicas:**

Ingeniería social	Usa el engaño para **manipular a un individuo para divulgar su información personal** y confidencial con propósitos de fraude. Esto incluye marcaciones por teléfono y chats en línea.
Motores de búsqueda	Son programas que navegan en la web de una manera metodológica y automatizada, los cuales **se usan para buscar información sobre compañías, personas y servicios.**
Redes sociales	Usan las **plataformas web para construir perfiles** y así llegar a los datos del usuario objetivo.

RECOPILACIÓN DE LA INFORMACIÓN

Metodología

La recopilación de información **se divide en siete pasos lógicos,** los cuales son:



- **Reunión** de la información disponible de la compañía y sus capacidades computacionales.
- **Reconocimiento** de las direcciones de red disponibles.
- **Identificación** de los equipos de los usuarios.
- **Descubrimiento** de los puntos de acceso y puertos abiertos de la red.
- **Detección** de los sistemas operativos usados.
- **Destape** de servicios de red y puertos ocultos.
- **Mapeo** de los equipos que componen la red empresarial.

Footprint puede además revelar las vulnerabilidades del sistema e identificar la facilidad con la cual se explotan.