**TEMA 2**

Independientemente de la anatomía de un ataque o kill chain que se utilice como referencia, existe un conjunto de técnicas que siempre se utiliza en las primeras fases: las que permiten recoger información y preparar las siguientes fases. La recogida de información suele dividirse en dos fases diferentes en función del tipo de técnica utilizada:

* Footprinting: Técnicas no invasivas, legales y fuentes públicas.
* Fingerprinting: Técnicas invasivas, alegales, información no pública.

Técnicas de footprinting:

* HUMINT
* IMINT
* GEOINT

Los buscadores nos pueden ayudar a encontrar:

* Ficheros con información sensible o útil.
* Directorios y contenidos.
* Nombres de usuario y contraseñas.
* Mensajes de error con trazas que proporcionen datos interesantes.
* Servidores con vulnerabilidades conocidas.
* Portales de login.

Para sacar el máximo partido a un buscador, si conoces la sintaxis como los Google dorks, palabras clave que permiten refinar la búsqueda.

* inurl: especifica que la cadena buscada debe aparecer en la url.
* intext: especifica que la cadena buscada aparezca en el cuerpo de la página.
* site: especifica que la cadena previa al dork aparezca en el sitio web especificado.
* filetype: sirve para especificar la extensión de los ficheros.
* link: sirve para localizar webs que tienen enlaces que dirigen a una página concreta.
* “” (comillas): la cadena que aparezca entre comillas debe aparecer exactamente en las páginas mostradas en los resultados.
* \* (asterisco): sustituye a cualquier palabra, pero sólo una.
* . (punto): sustituye a una o varias palabras.
* and, not: operadores lógicos.
* +, -: inclusión y exclusión de resultados (es decir, filtros).

Shodan es un buscador de dispositivos conectados a Internet. Nos puede ayudar a encontrar:

* Dispositivos de un tipo concreto (PLC, cámara de vídeo, router).
* Dispositivos de un modelo concreto.
* Dispositivos en una zona geográfica concreta.
* Dispositivos con un software o S.O determinado instalados.
* Dispositivos con una determinada dirección IP o con cierto puerto abierto.

METADATOS

” Datos sobre los datos”, es decir, información públicamente accesible sobre determinados datos de un documento, una dirección IP… Pero también de información acerca de workstations, servidores o impresoras. Hoy en día, incluso información de geolocalización.

OTRAS FUENTES ABIERTAS DE INTELIGENCIA

En ocasiones es muy útil copiar el código fuente completo de una web y descargar todos sus archivos asociados. Esto permite un análisis estático en profundidad y una búsqueda muy completa de cierto tipo de información y vulnerabilidades. A veces se encuentran rutas absolutas, nombres de usuario o de host e incluso contraseñas. El comando **wget** es muy útil en este sentido.

Otra fuente de información muy útil es el protocolo DNS. El comando **whois** permite obtener información sobre un dominio concreto.

La herramienta host permite resolver un nombre DNS a IP o viceversa. También permite hacer una transferencia de zona completa, de manera que se descargue la información de todos los hostnames de un servidor DNS en concreto.

\*NOTA: para ver la IP de un nombre de dominio: host [nombre.dominio]

Para ver quien esta autorizado a mandar correos a nombre de [nombre.dominio]: Si sabes quién está autorizado, puedes identificar rápidamente correos fraudulentos que intentan hacerse pasar por tu dominio

Texto

Descripción generada automáticamente

Todos los servidores que se encuentren en spf.eforw.com estarán autorizados para mandar mails a numa.host

Otra actividad que puede resultar muy útil en la fase de recogida de información de un ataque puede ser dibujar la red e identificar los dispositivos intermedios entre el atacante y la víctima. Por ejemplo, utilizando el comando **ping**.

También puede ser útil trazar el camino que sigue la información desde nuestra máquina hasta la máquina de destino. Con esto podemos obtener direcciones IP, identificar puertas de enlace, firewalls, etc. Ejemplos de comandos útiles son: traceroute, tcptraceroute, tctrace, intrace…