Footprinting

Mayo 2015

¿Qué es Footprinting?

- En un ataque o intrusión…
- Es el primer paso para obtener información sobre una red y su ambiente (pre-ataque)
- Mediante el footprinting es posible encontrar varias formas de entrar a una organización

Footprinting

- La información recolectada puede ser pública o privada
- Muchas veces se tiene acceso a la información privada debido a una mala configuración
- El footprinting intenta obtener la mayor cantidad de detalles sobre el objetivo
- El atacante pretende conocer y aprender mejor su entorno
  - Por ejemplo: Empleados, sistemas, políticas, clientes, proveedores, sucursales.
- Es una etapa vital en el proceso global de penetración
- Si es posible conocer cada detalle del objetivo habrá más oportunidad de lograr ataques eficientes y exitosos

Información recolectada

- Sistemas operativos utilizados
- Plataformas en ejecución
- Versiones de los Servidores Web
- Utilizar técnicas como: whois, dns
- Encontrar vulnerabilidades

¿Porqué el footprinting?

- Conocer el perfil de la organización (respecto a seguridad)
- Reducir el área de ataque (conocer nombres de dominios, bloques de redes, ip individuales)
- Construir bases de datos (objetivos encontrados en la organización)
- Crear diagramas de red de la organización

Encontrando URLs Internas/Externas

- Utilizar motores de búsquedas (Google, Bing)
- Prueba escribiendo el nombre del objetivo
- Analiza la información mostrada por los motores de búsquedas

Ejemplos de Búsquedas

- Google Hacking | Google Operadores
  - Se puede utilizar para encontrar vulnerabilidades en páginas web
  - Se filtra información
  - Implica el uso de operadores avanzados
- Google Dorks
  - filetype:pdf
  - intitle:"Index of /" site:"www.cobaev.edu.mx"
  - intitle: “Live View /- AXIS”

Operadores de búsqueda

Operador	Propósito
intitle	busca paginas con ese titulo.
allintitle	busca paginas que solamente tenga ese titulo en especifico.
inurl	busca direcciones en Internet que tengan ese URL.
allinurl	busca direcciones en Internet solamente las paginas que tengan ese URL.
filetype	especifica un tipo de extension de archivo.
allintext	busca solo ese texto en especifico.
site	busca una especifica pagina en Internet.
link	busca las paginas relacionadas con esta frase.
inanchor	busca el texto anchor de la pagina relacionada.
daterange	busca un rango de datos.
author	busca un grupo de autores.
group	busca el nombre de algún grupo.
insubject	busca un tema en particular.
msgid	busca el grupo msgid.

Whois

- Protocolo TCP basado en petición/respuesta utilizado para efectuar consultas en una base de datos que permite determinar el propietario de un nombre de dominio
  - http://whois.net/search/

Actividad en clase

- Elegir un sitio Web y crear un reporte que contenga información detallada del sitio objetivo
- Utiliza motores de búsquedas entre otras herramientas para conocer información detallada del objetivo
  - ¿Quién tiene registrado el nombre del dominio?
  - ¿Dónde se encuentra?
  - ¿Cuáles son los servidores de dominio?
  - ¿Qué servicios tiene instalado?