UNIVERSIDAD AUTÓNOMA DE CHIAPAS

LICENCIATURA EN INGENIERIA EN DESARROLLO Y TECNOLOGIAS DE SOFTWARE

Unidad académica: Análisis de Vulnerabilidades

Actividad: Cuadro Comparativo de Footprintig

Grado: 7 Grupo: M

Alumno: Abel Alejandro Jimenez Camacho

Matricula: A170147

¿Qué es el footprinting?

Es un proceso en el cual se recoge toda la información posible sobre el objetivo en cuestión, para intentar encontrar una posible forma de acceder a un sistema. Es una técnica pasiva, es decir, en ningún momento se interactúa de manera directa con el objetivo, únicamente se recolecta información ya sea de fuentes públicas o privadas, pero sin llegar a más, por ejemplo, un escaneo de puertos no sería posible.

Es un proceso que requiere de tiempo y paciencia, ya que se trata de perfilar a la organización objetivo, recopilando información sobre altos cargos, la red, y las personas relacionadas con la organización.

Se recopila información como la dirección IP, registros Whois, información del DNS, direcciones de correo electrónico de empleados, números de teléfono, etc.

¿Para qué es útil?

Cuanto más se sepa sobre el objetivo mejor, así se le podría hacer un ataque a medida. Los grandes ataques de ransomware se deben a un gran perfilado de la compañía. Detectan al eslabón más débil para poder desplegar el ataque y así lograr que su objetivo, que en este caso sería el de secuestrar todos los datos del objetivo, logrando paralizar prácticamente por completo toda actividad, véase el caso de la empresa Damm (dedicada a la elaboración de cerveza), que debido a un ataque de ransomware ha tenido que parar la producción en la fábrica del Prat de Llobregat.

Aquí se puede ver la importancia de un buen footprinting, que, aunque no lo parezca, puede ser una de las fases más importantes a la hora de un ataque.

Técnicas de footprinting

Búsqueda

Todo comienza con una simple búsqueda desde nuestro navegador. Vamos a suponer que queremos obtener información sobre Exploitables, pues es tan fácil como buscar en internet y ver que hay. Podremos ver que Google muestra resultados relacionados con esa palabra, y de ahí podremos sacar páginas asociadas con información (relevante o no), tal vez algún email, algún formulario de contacto, tal vez algún archivo, en definitiva, la búsqueda puede parecer simple, pero de ahí podemos obtener información que nos ayudaría a realizar un ataque de ingeniería social.

Google Dorks / Google Hacking

Sin entrar en demasiadas explicaciones, los Google Dorks son cadenas de búsqueda que usan operadores de búsqueda avanzada para encontrar información que no es tan fácilmente accesible. Se puede obtener información que

no está pensada para mostrarse de manera pública, pero que no ha sido bien protegida, debido a una mala configuración de un sitio web.

Búsqueda en Redes Sociales
Es muy importante analizar las redes sociales para obtener información sobre un objetivo. Es muy útil de cara a obtener información sobre empleados de una empresa, tecnología que utilizan, etc. Los Google Dorks pueden hacer que la búsqueda de posibles datos en las redes sociales sea más sencilla, por ejemplo, site: twitter.com, site: facebook.com, etc. este dork devolverá toda la información indexada sobre el objetivo que esté en Twitter y Facebook. Este dork se puede adaptar a la gran cantidad de redes sociales, tan solo hay que cambiar el nombre de la red social en el apartado de site.

Portales de trabajo
Este tipo de sitios webs es un recurso valioso para lograr identificar las tecnologías utilizadas por una empresa que tengamos como objetivo. Podemos usar Google Dorks para obtener información de manera más eficiente, como, por ejemplo: sitio: indeed.com

Es un paso importante que no se suele tener en cuenta pero que a veces puede ser muy útil.

WHOIS
Indispensable para obtener información relacionada sobre el dominio registrado y las personas involucradas en el registro de este mismo. Es muy interesante de cara a un ataque de ingeniería social, por ejemplo, contactando a algún gestor del registro de dominio para comunicar una falsa incidencia, a ver qué datos que no están publicados de manera directa podemos obtener.

Netcraft
Similar al WHOIS pero arroja aún más información sobre el sitio web, como por ejemplo, la tecnología que utiliza el sitio web. Probad con alguna web y veréis lo que podéis obtener gracias a esta interesante herramienta.

DNS Recon
Gran herramienta enfocada al reconocimiento DNS como su propio nombre indica. Una vez que ya tenemos DNS Recon en nuestra máquina, lo primero es ejecutar el siguiente comando dnsrecon -w
-w se encarga de iniciar un análisis de registros WHOIS profundos. DNS Recon proporcionará el registro WHOIS, las direcciones de host, los servidores de nombres y las direcciones IP, así como los registros de correo MX y otra información DNS.

theHarvester
Se puede recopilar información como puede ser: correos electrónicos, subdominios, hosts, nombres de empleados…
Para ejecutar esta herramienta es necesario escribir en el terminal lo siguiente:

theHarvester -d -l -b -f
Con este comando obtendremos toda la información recopilable por parte de theHarvester, guardará esta información en un fichero .xml, adjunto foto de la información que consiguió con mi búsqueda: