Maltego TC2027

27 enero 2017

Gustavo Francisco Méndez De La Cruz– A01332475
a01332475@itesm.mx

La siguiente práctica se tratará de la herramienta de maltego, en la cual el alumno será capaz de utilizar la herramienta, identificar lo siguiente:

- Dominio
- DNS (Domain Name Scheme)
- Mail ExChanger
- Name Server
- IP Address
- Geographical Location
- Identidades
- Transforms
- Encontrar un mail y un número.

El siguiente documento se hizo para el laboratorio de seguridad informática con el propósito de conocer y utilizar la herramienta de Maltego, hecha por Paterva.

Se necesitará Kali Linux

Secciones

Website

Abrir Maltego. Saltar todas las instrucciones, si es posible poner el botón cancel. Del lado izquierdo en la parte superior insertar nueva gráfica.

En la paleta del lado izquierdo abrir donde dice Infrastructure, y arrastrar website, a la website le pondremos lo siguiente: www.tec.mx

Seleccionaremos **Run Transform → All Transforms → To Server Technologies**

Lo que se hará es ver todas las tecnologías en las que trabaja esa página web.

También si ponemos **Run Transform → All Transforms → ToTrackingCodes.**

Podemos ver su Google Id Analytics y si ponemos toDns podemos ver el domain name server.

Y después en el resultado de toDNS, en el Domain Name Server igual hacer click derecho y aplicar **Run Transform → All Transforms →to DNS Name – Mx**. Este regresa el nombre del servidor del mail. Con esto los atacantes lo utilizan para explotar vulnerabilidades en el servidor, y por ende realizar actividades maliciosas como correo spam.

También en la entidad del resultado de toDNS poner el transform que **Run Transform → All Transforms →to DNS Name (Name Schema)** Con esto se puede simular varias técnicas de explotación para ganar información sensible. Por ejemplo tratas de entrar a ese servidor a partir de un diccionario o fuerza brutra.

Y por último poner **Run Transform → All Transforms →to DNS Name – NS,** y nos regresará el nombre del servidor principal, por lo tanto con esta información el atacante puede hacer DNS Hijacking y redirección de urls.

Otra cosa que se puede hacer es que en la entidad principal podemos poner **Run Transform → All Transforms →to IP Address DNS.**
Con esto se puede conocer el ip address, y ver con nmap que puertos están abiertos, para ver así sus vulnerabilidades, para ingresar a la red.
Del resultado anterior aplicamos lo siguiente con click derecho **Run Transform → All Transforms →to location**

A partir podemos ver en donde se encuentra el servidor donde está la IP Address.

Ahora en el resultado de toDNS, das click derecho y aplicas lo siguiente **Run Transform → Domain Owner Detail →To Entities (NER)**

Mail

Ahora hacemos una nueva gráfica, y en la paleta del lado izquierdo abrir donde dice personal, y arrastrar person, a person le pondremos lo siguiente David Zarate Trujillo y aplicar lo siguiente
Run Transform → All Transforms →To Email Address (Verify Common)

También podemos hacer lo siguiente poner

Run Transform → All Transforms →To Phone Numbers