theHarvester Ver. 3.0.6 Coded by Christian Martorella
Edge-Security Research cmartorella@edge-security.com

Enlace de descarga de github:https://github.com/laramies/theHarvester

TheHarvester, fue creado con la finalidad de usarse en la fase mas importante en el paso de un pentester, esta fase es la de recolectar informacion, y theharvester tiene la fortaleza de obtener informacion muy relevante como por ejemplo email, subdominios,URL,ip, entre otros utilizando varias fuentes publicas.con esta herramienta podrán seguir reforzando su diccionario de palabras recolectada anteriormente.

Nota importante: theharvester es muy poderoso pero lamentablemente es muy probable que después de que realicemos nuestro primer análisis, posiblemente GOOGLE bloquee su ip de manera temporal y tendrán que esperar al menos 2 o 3 horas, para realizar nuevamente otro análisis

Recomendación: pueden busca algún dominio de empresas grandes como universidades, hospitales, escuelas entre otros para obtener buenos resultados y comprender el funcionamiento.

Uso: las opciones del recolector

-d: dominio para buscar o nombre de la empresa

-b: fuente de datos: baidu, bing, bingapi, censys, crtsh, dogpile,
google, google-certificados, googleCSE, googleplus, google-profiles,
cazador, linkedin, netcraft, pgp, grupo de amenaza,
twitter, vhost, virustotal, yahoo, todos

-g: usa Google Dorking en lugar de la búsqueda normal de Google

-s: comienza en el número de resultado X (predeterminado: 0)

-v: verifica el nombre del host a través de la resolución DNS y busca hosts virtuales

-f: guarda los resultados en un archivo HTML y XML (ambos)

-n: realiza una consulta inversa DNS en todos los rangos descubiertos

-c: realiza una fuerza bruta de DNS para el nombre de dominio

-t: realizar un descubrimiento de expansión de DNS TLD

-e: usa este servidor DNS

-p: el puerto escanea los hosts detectados y comprueba las adquisiciones (80,443,22,21,8080)

-l: limita el número de resultados con los que trabajar (Bing va de 50 50 a resultados,

Google 100 a 100, y PGP no usa esta opción)

-h: utiliza la base de datos SHODAN para consultar hosts descubiertos

Ejemplos:

theharvester -d microsoft.com -l 500 -b google -f myresults.html

theharvester -d microsoft.com -b pgp, virustotal

theharvester -d microsoft -l 200 -b linkedin

theharvester -d microsoft.com -l 200 -g -b google

theharvester -d apple.com -b googleCSE -l 500 -s 300

theharvester -d cornell.edu -l 100 -b bing -h

Para invocar eta herramienta debemos teclear en una consola el siguiente comando:

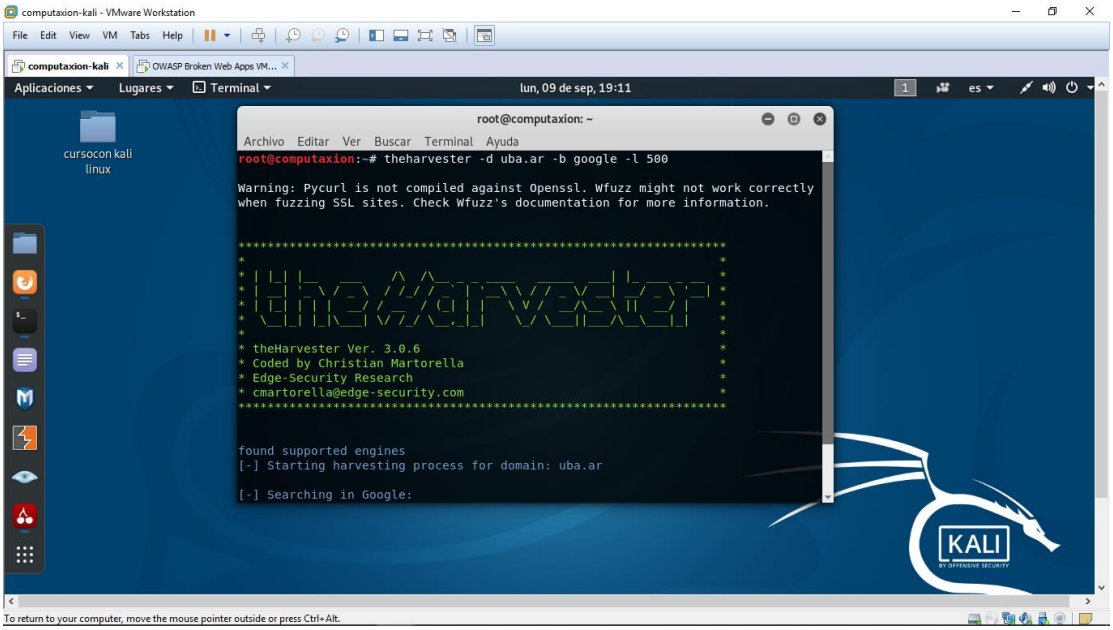
root@computaxion:~# theharvester -h

Este comando aparte de traernos la herramienta en la consola, nos muestra la ayuda, lo cual se darán cuenta que es muy intuitiva y fácil de comprender, y también nos muestra varios posibles comandos a ejecutar.

Bien ahora es importante aclararles que esta herramienta buscara en el objetivo a analizar TODA LA INFORMACION PUBLICA QUE PUEDA ENCONTRARSE DENTRO DE INTERNET. Por lo tanto no se constituye como algo ilegal, o un delito informático, cabe destacar que se puede encontrar informacion de terceros dentro de un análisis por ejemplo email o subdominios ajenos al objetivo, pero contratados por los mismos, con esto me refiero a que pueden encontrar informacion de empresas que brindan servicios para la misma, como por ejemplo algún antivirus, o software de microsoft etc, ese tipo de informacion ustedes las tienen que obviar por que no se los contrato para realizar un análisis a esos servicios, aparte seria perder dinero en tiempo. :) .

El comando que vamos a usar para ver los resultados es el siguiente:

root@computaxion:~# theharvester -d uba.ar -b google -l 500



material para las próximas clases: OWASPBWA https://sourceforge.net/projects/owaspbwa/