Utilizando The Harvester para analizar el riesgo de la información pública

The Harvester es una herramienta para recolectar información publica en la web. Aprende cómo funciona para anticiparte a ataques de Ingenieria Social.

Uno de los problemas más habituales en empresas es la fuga de información. Pero cuando hablamos de ello no solamente nos referimos a filtrado de archivos o información confidencial; existen también, por ejemplo, direcciones de correo electrónico que **no deben ser publicadas** abiertamente. Esto permitiría a los ciberdelincuentes, de manera fácil y efectiva, enviar ataques personalizados por correo electrónico a todo el personal, aumentando la superficie de ataque y las probabilidades de éxito.

En este post veremos una herramienta que se vale de información pública en buscadores, para encontrar este tipo de información. **The Harvester** fue desarrollada por Christian Martorella, quien trabaja para la empresa Edge-Security.

Si bien ya hemos visto herramientas para recolección de información como Maltego, en esta entrada veremos otra alternativa libre y gratuita.

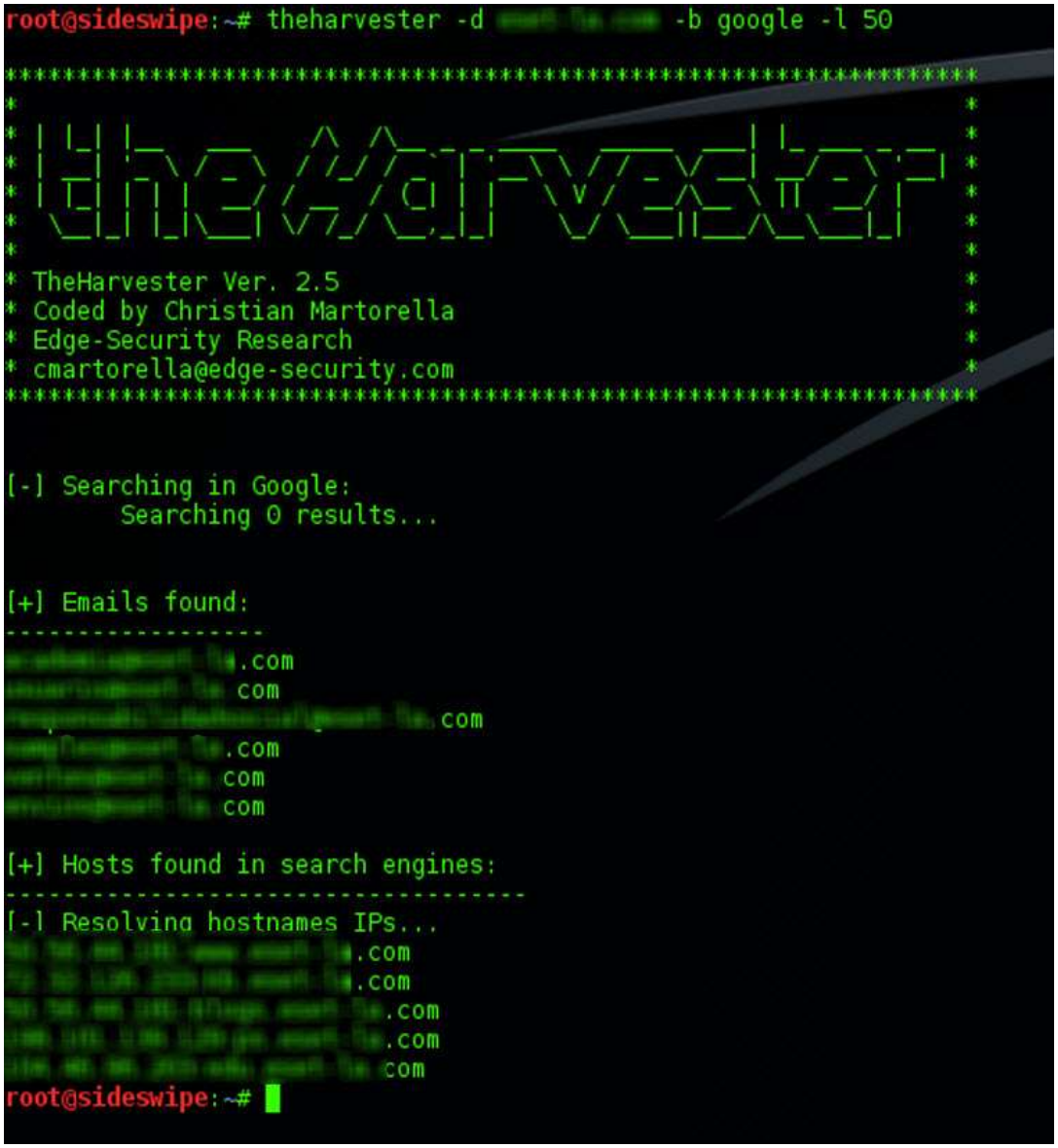
Esta *tool* viene incluida en las distribuciones de Linux tales como Kali y Bugtraq entre otras, y también se puede descargar desde su repositorio en GitHub para su instalación. Una vez realizada la instalación, basta con invocarla desde **consola** con su nombre para obtener el menú de ayuda.

A continuación pueden ver la ejecución del comando:

Comando: theharvester

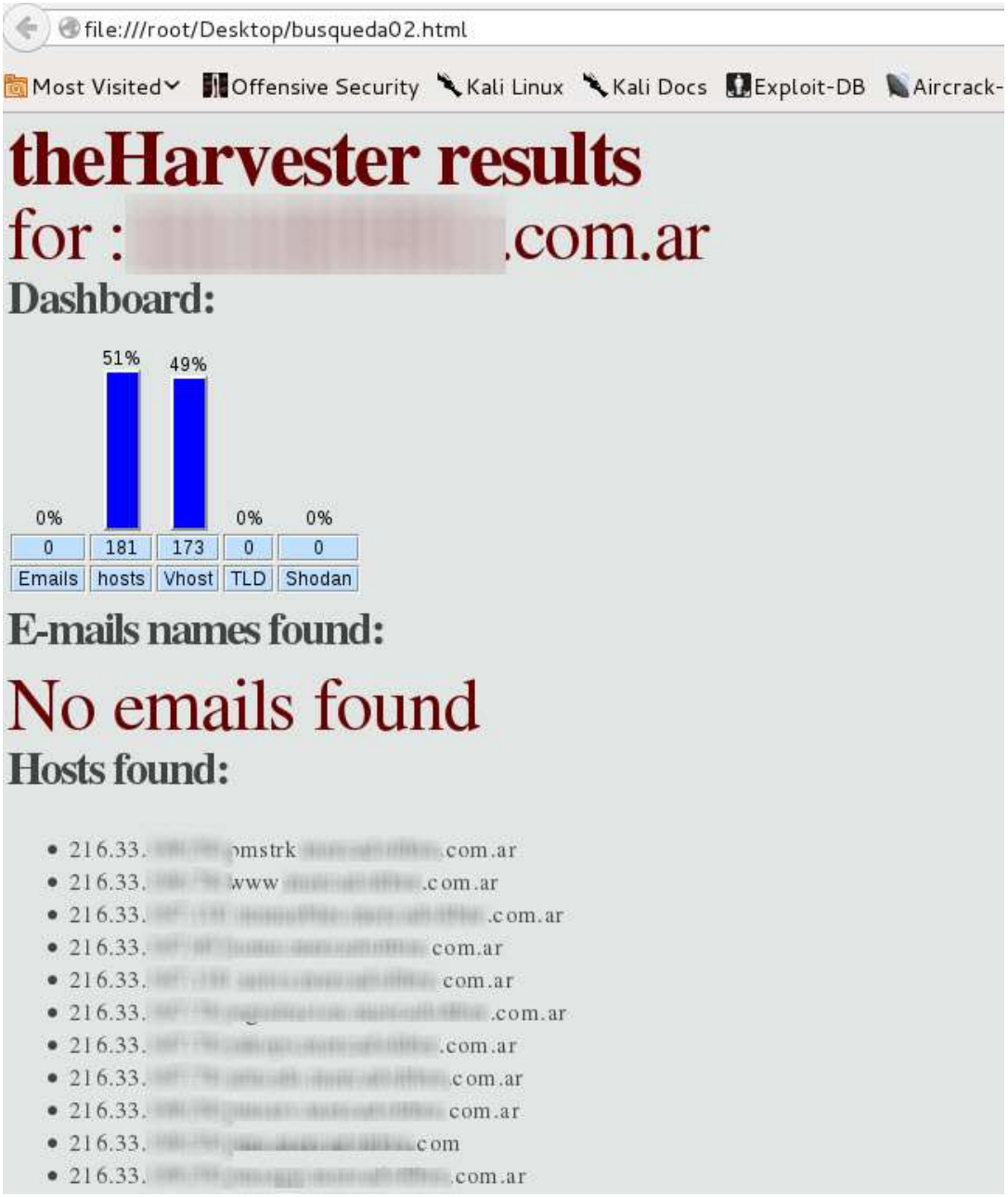
Como se muestra en la captura de pantalla anterior, permite la ejecución de diferentes parámetros para refinar la búsqueda de información. No entraremos en detalle respecto a cada uno de estos parámetros, ya que el menú de ayuda posee la descripción de la función que ejecutan.

The Harvester puede ejecutarse de forma tradicional por consola, obteniendo resultado en la misma como se muestra a continuación:

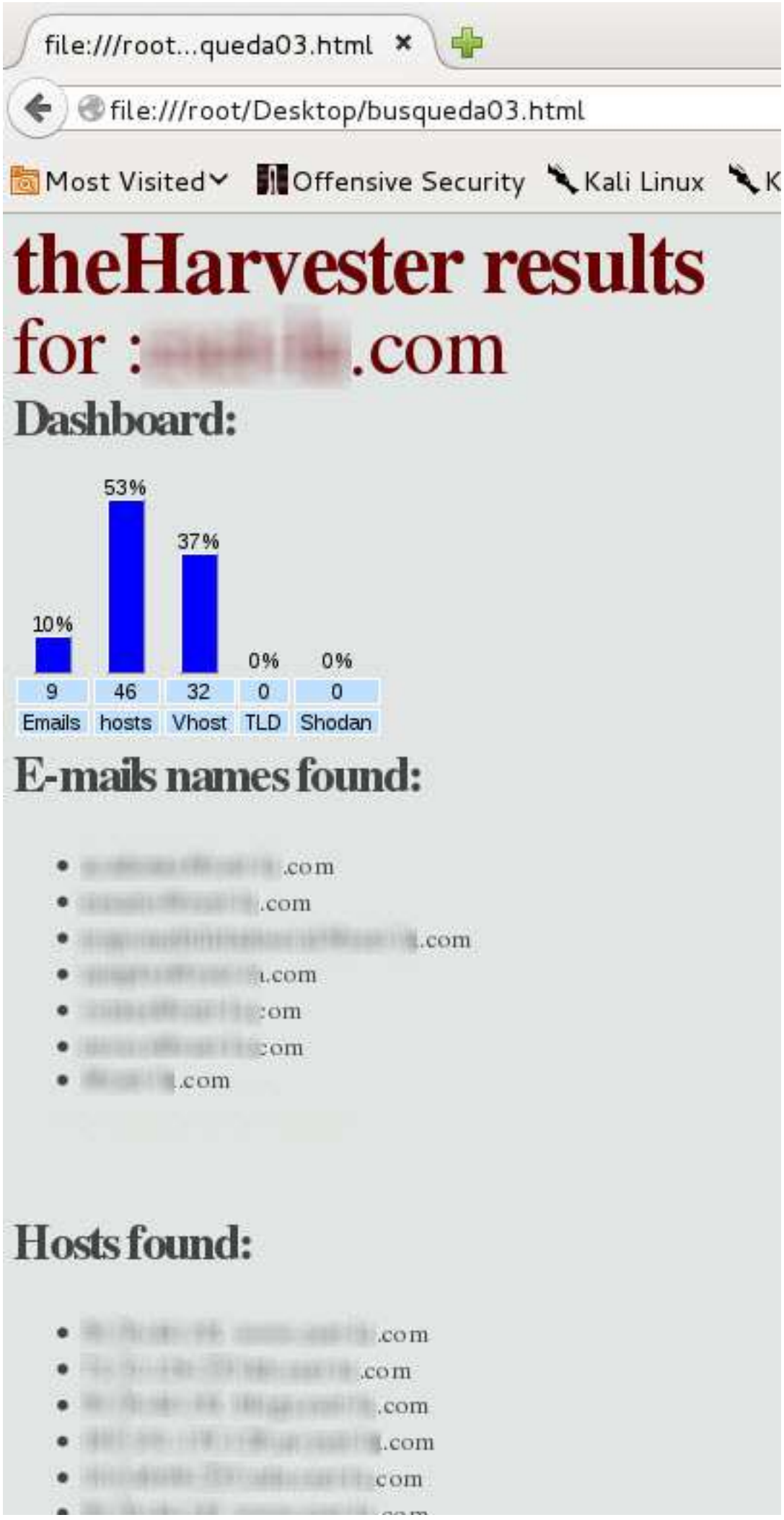


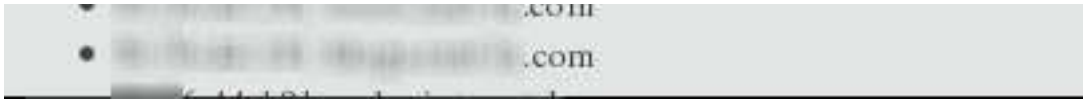
Aunque una de las funcionalidades más interesantes es que permite **exportar los resultados** de cada búsqueda a archivos HTML y XML (esto lo realiza agregando el parámetro –f nombre_de_archivo) permitiendo la automatización en procesos de auditoría. Muchas de estas *tools* admiten **importar** este formato de archivos para usar sus resultados obtenidos en otras herramientas.

También es muy útil para la elaboración de informes al finalizar dicha auditoría. A continuación vemos una captura de un informe en HTML:



En este primer informe, puede verse que en la búsqueda realizada a modo de ejemplo (decidimos preservar la identidad de la empresa por motivos de seguridad) no se encuentran correos electrónicos públicos. Mientras que en la búsqueda que mostraremos a continuación, **puede verse claramente que sí, y cuáles son:**


file:///root...queda03.html
file:///root/Desktop/busqueda03.html
Most Visited
Offensive Security
Kali Linux
theHarvester results
for : [redacted].com
Dashboard:
10%
53%
37%
0%
0%
9
46
32
0
0
Emails
hosts
Vhost
TLD
Shodan
E-mails names found:
[redacted].com
Hosts found:
[redacted].com



Si bien hay direcciones que deben ser públicas, normalmente las que corresponden a servicios pensados para la comunidad, hay otras que no deberían estar al alcance de un buscador. El motivo es la seguridad de los datos, naturalmente, pero si todavía te sigues preguntando por qué y cómo el hecho de que sean públicas podría ser un problema, analicemos la siguiente situación:

¿Qué sucede si un cibercriminal decide realizar un ataque dirigido a una empresa?

Imaginemos que en su fase de reconocimiento y búsqueda de información, encuentra pública en Internet una lista con todas las direcciones de correo electrónico de la compañía víctima. Esto le permite crear una lista, a la cual luego podría enviar correo **masivamente** con algún *malware* mediante Ingeniería Social. No olvidemos que el *phishing* y otras viejas amenazas siguen siendo una preocupación en las empresas.

La superficie de ataque y las probabilidades de tener éxito serán mucho mayores que en los ejemplos mostrados en las capturas, debido a que esto le llegaría a mayor cantidad de usuarios, convirtiéndose en una campaña que podría comprometer la red –solo con que alguien haga clic en el **correo equivocado**.

Entonces, repasando y resumiendo la situación, aparte de las soluciones de seguridad, políticas y recaudos, es completamente necesaria la proactividad de analizar el nivel y la superficie de exposición tanto de la empresa como de sus usuarios. Como siempre recomendamos, la educación a los usuarios facilitará que estos se conviertan en un aliado y no en el enemigo dentro de la empresa.

Créditos imagen: ©David Wright/Flickr
8 Apr 2015 - 12:04PM

Newsletter