PENTESTING PLAYGROUND 101

Alumno: Danny Mogrovejo Gonzales

Ejercicios

1. Identificar 5 subdominios de la página de Coca Cola (Coca-Cola.com) - Buscar con comando de Google Hacking

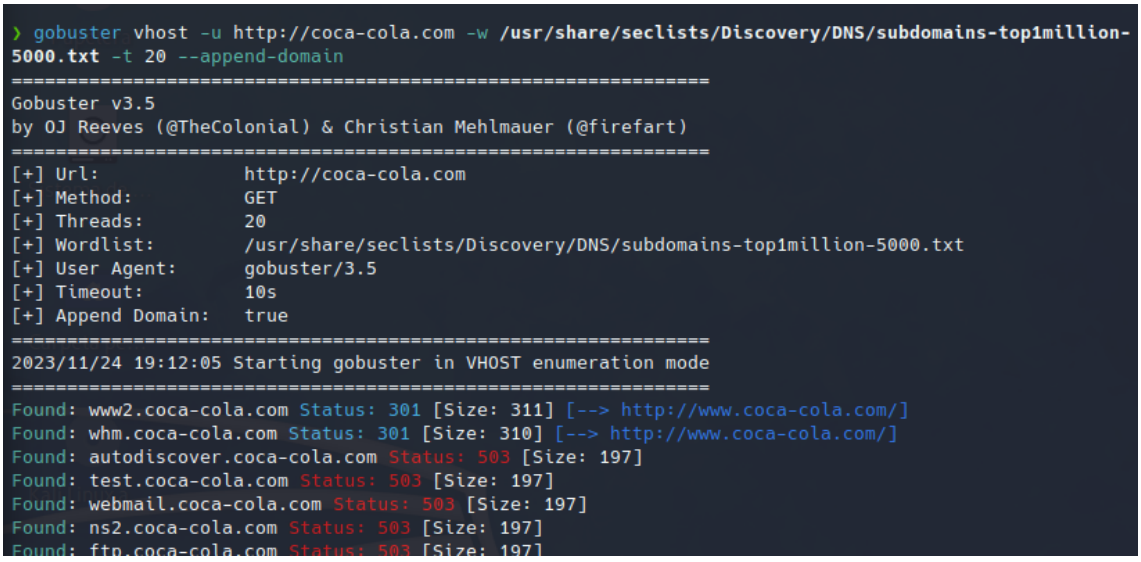
   Para poder ejecutar una búsqueda de subdominios desde GoogleHacking, para la página de Coca Cola, lo primero que haremos será utilizar el parámetro "Site:" además de a continuación usar el parámetro *, de modo tal que se puedan encontrar posibles subdominios a partir de colocar a continuación el nombre de la página como se muestra a continuación:

   Buscamos en Google: **Site:*.coca-cola.com**

   Lo cual nos entrega como resultado algunos de los siguientes subdominios

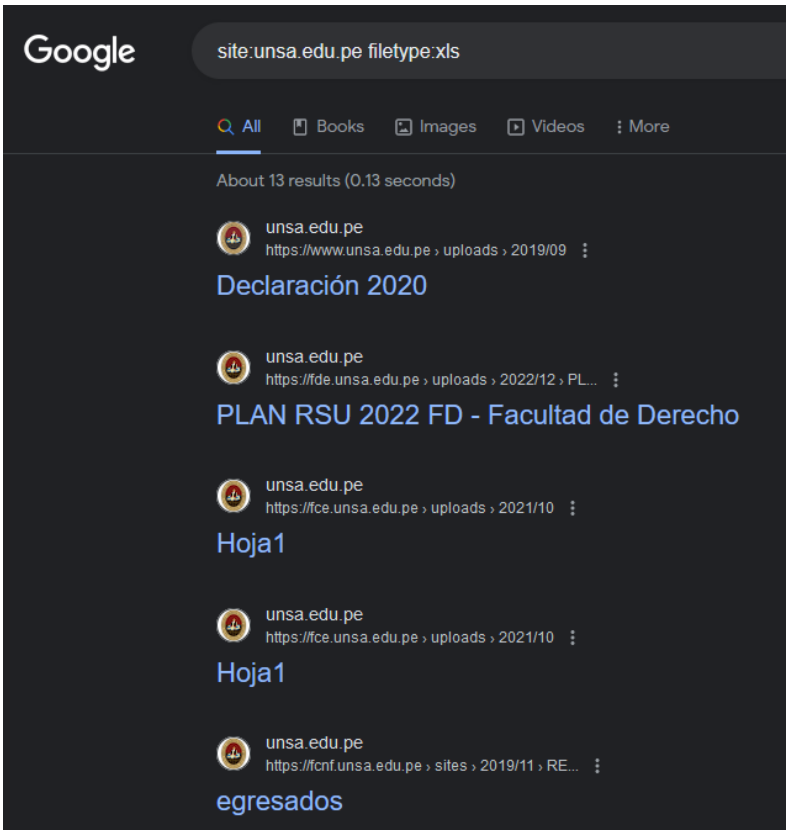
   - https://crewconnect.coca-cola.com/
   - https://dunkinanytime.coca-cola.com/faqs
   - https://clientes.coca-cola.com/
   - https://mv.coca-cola.com/en/history
   - https://summerrefreshment.coca-cola.com/

   Además, también podemos hacer uso de la herramienta Gobuster en Kali Linux para el descubrimiento de subdominios, a través de diccionarios específicos que se le entrega a la herramienta y buscará de una manera más enfocada.



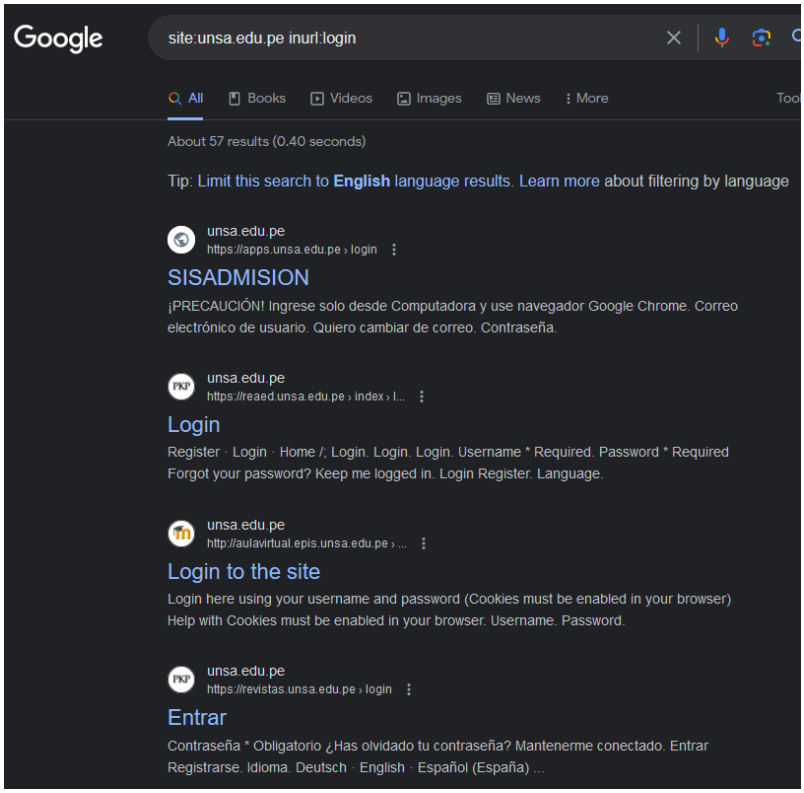
2. Busque documentos de tipo excel de cualquier organización

   Utilizando el comando **"Site:"** para especificar la organización y el comando **"Filetype:"** para especificar el tipo de documento que estamos buscando, hacemos la siguiente búsqueda



3. Identifique algún login de intranet de cualquier empresa

   A través el uso del siguiente comando site:unsa.edu.pe inurl:login, se puede visualizar el tipo de salidas



4. Busque su nombre con Google Hacking, ¿Qué encontró?

   Haciendo únicamente uso de las comillas dobles he ingresando mi nombre completo, por suerte pude verificar que no es posible encontrar información muy personal de parte mia, mas que información profesional, que a fin de cuentas es información que en parte si me agrada que sea de manera pública.

5. Encuentre páginas hackeadas de su gobierno

   Hace unos 8 años aproximadamente, en fechas del aniversario del Perú, la página web del gobierno peruano www.peru.gob.pe fue hackeada por un grupo de hackers chilenos, sin mas consecuencias en realidad que la de tratas de hacer burla de la seguridad del sitio y cambiando algunos de los códigos fuente de la página web. Colocaron mensajes como el siguiente “El pueblo no debe temer a sus gobernantes, los gobernantes deben temer al pueblo”

6. Encuentre 3 correos expuestos de la organización que desee (Buscar correos electrónicos expuestos en páginas de organizaciones)

   institucional@ucsp.edu.pe
   rsu@ucsm.edu.pe
   ouis@unsa.edu.pe

   Son correos públicos expuestos en 3 organizaciones que han sido vulnerados según HaveIbeenpawnd.com