Práctica de laboratorio: Información sobre la organización

Objetivos

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Encuentre información sobre violaciones al correo electrónico.
- Vea los metadatos del archivo.

Aspectos básicos/Situación

El propósito del reconocimiento en la prueba de penetración es recopilar información sobre un cliente que se puede usar más adelante para su explotación. Hay muchos recursos que ayudan con este proceso. En esta práctica de laboratorio, aprenderá sobre recursos en línea que pueden proporcionar información sobre una empresa.

Recursos necesarios

- Kali VM personalizada para el curso de Ethical Hacker
- Acceso a Internet

Instrucciones

Parte 1: Encuentre información sobre violaciones al correo electrónico.

Es posible obtener más información sobre una persona u organización mediante la búsqueda en una dirección de correo electrónico conocida. Es útil determinar si los empleados de una empresa han visto comprometidas sus direcciones de correo electrónico de trabajo. Varios servicios en línea brindan la capacidad de buscar en direcciones de correo electrónico individuales y dominios completos para revelar violaciones. Algunos de esos sitios son:

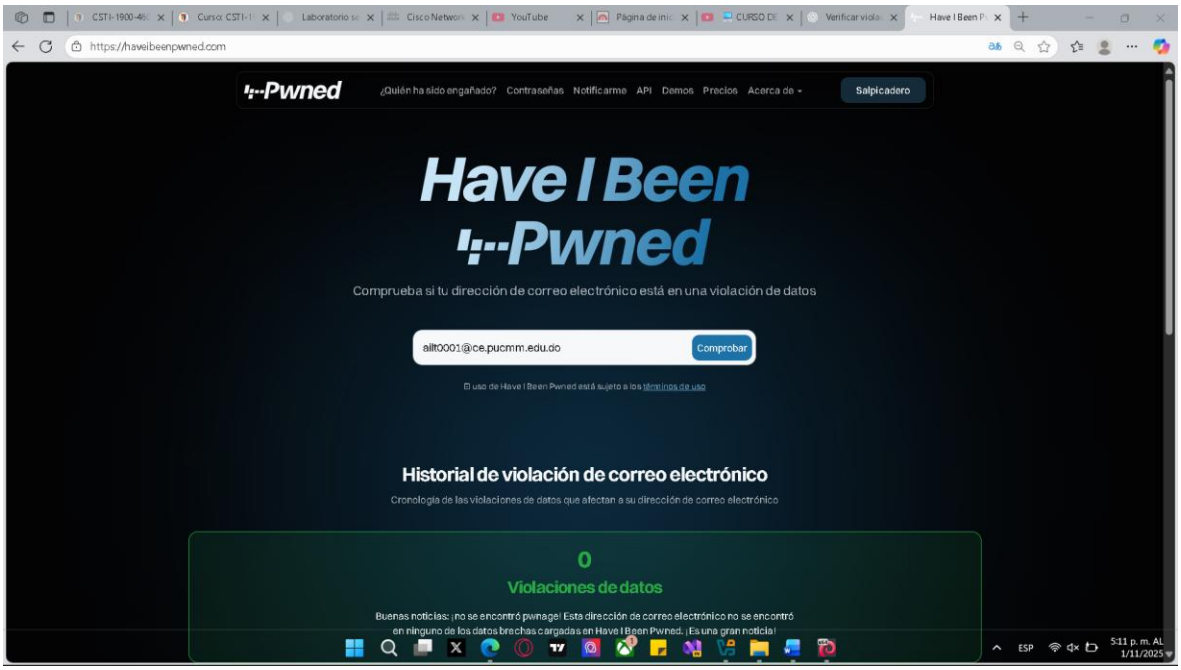
- haveibeenpwned.com
- f-secure.com
- hacknotice.com
- breachdirectory.com
- keepersecurity.com

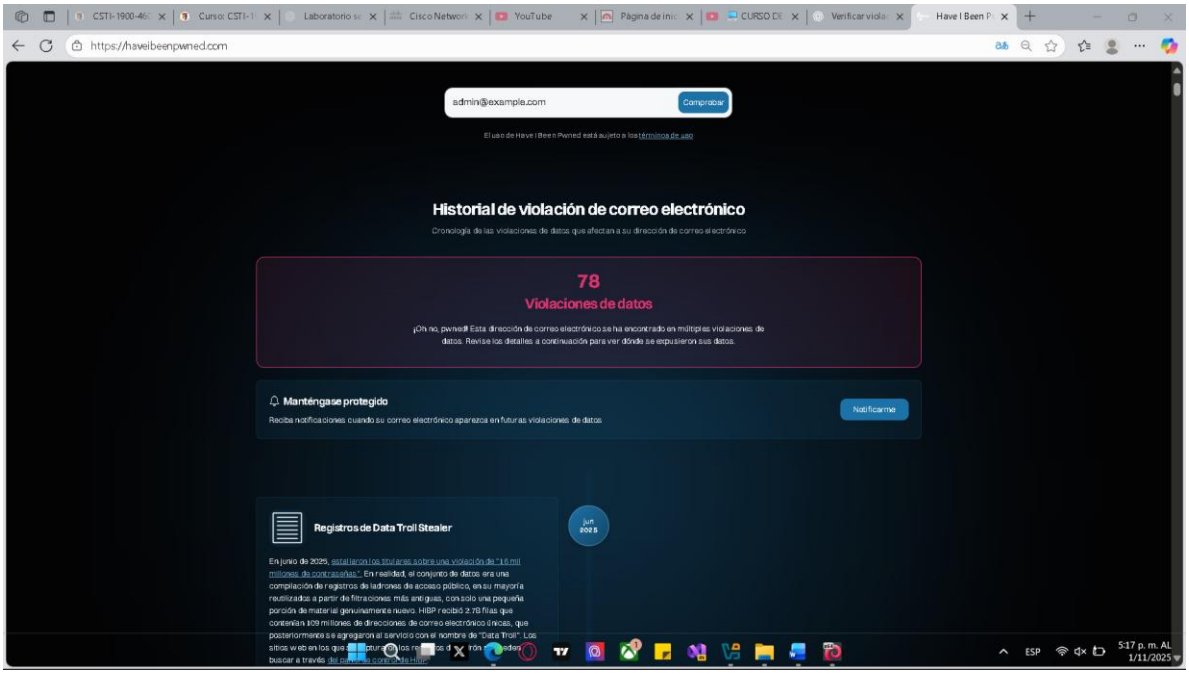
Paso 1: Investigue el estado de su correo electrónico.

Explore los diferentes sitios y busque su propia dirección de correo electrónico o el dominio de una empresa que conozca. Es especialmente preocupante si se ha producido una violación de datos reciente para un dominio. También es posible que un cliente de pruebas de penetración no tenga conocimiento de la violación.

Existen recursos que permitirán el acceso a estos archivos de violación de datos. Desde allí, puede encontrar nombres de usuario, direcciones de correo electrónico, contraseñas y otra información sobre los empleados. Esta información será muy útil en la parte de explotación del proceso de pruebas de penetracion.

¿Sus direcciones de correo electrónico han sido parte de una violación? Si es así, ¿en qué violación o violaciones se revelaron? **Nota: para esta parte es suficiente con usar haveibeenpwned.com nada más**



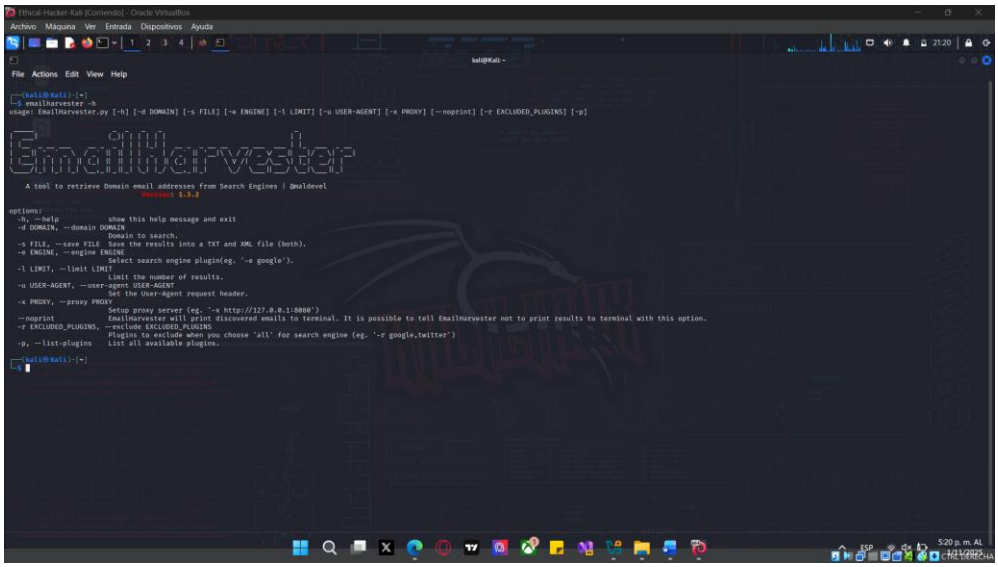


Paso 2: Use una herramienta para buscar direcciones de correo electrónico para un dominio.

Utilizará una herramienta llamada EmailHarvester para encontrar información sobre un dominio, incluidas las direcciones de correo electrónico del personal.

a. Abra una terminal e ingrese el comando **emailharvester**. La herramienta aún no se ha instalado en Kali, pero es parte del conjunto de herramientas de Kali. Ingrese **y** para aceptar la instalación de la herramienta y proporcione la contraseña para el usuario **kali** si se le solicita.

b. Una vez completada la instalación, use la opción **-h** para ver las opciones disponibles en la herramienta.



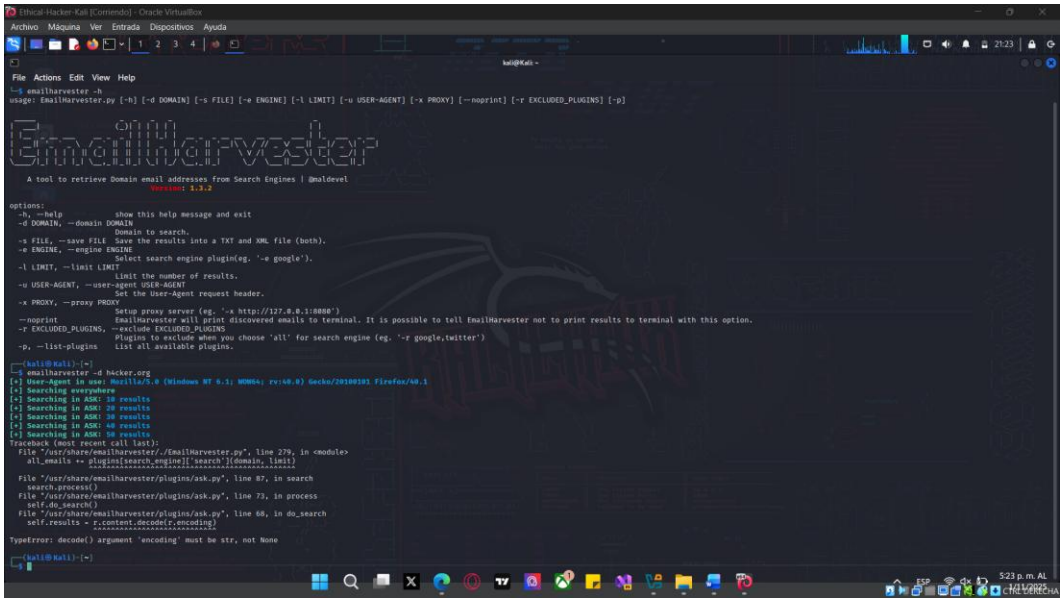
¿Qué hace la opción -d?

-d DOMAIN, --domain DOMAIN

Domain to search.

La opción -d es para escanear dominios.

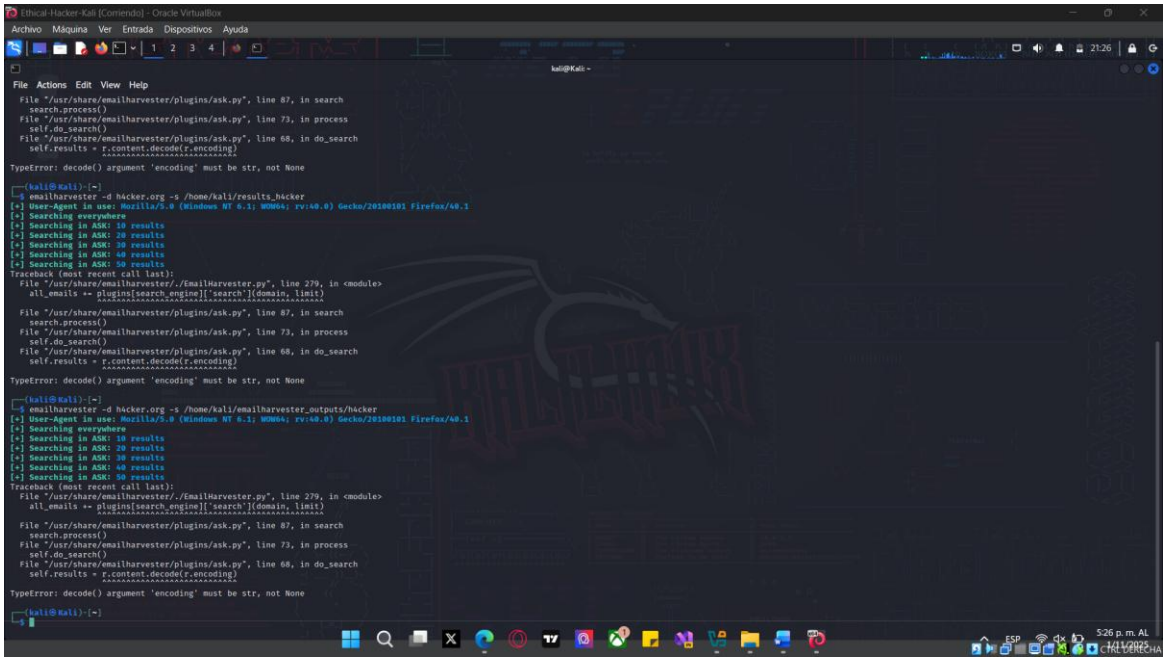
c. Investigue dominios como **h4cker.org**, **hackxor.net**y **scanme.nmap.org**. También puede probar otros dominios con los que esté familiarizado, siempre que no infrinja los términos de este curso. Por ejemplo, use el comando **emailharvester -d h4cker.org**.



d. Verifique algunas de las direcciones de correo electrónico que obtuvo para determinar si han sido parte de una violación de datos. Si es así, esto indica que los detalles de la cuenta están disponibles en la dark web. Un evaluador de penetración que tenga acceso a bases de datos de intrusiones podría buscar información adicional allí.

e. Los resultados pueden enviarse a un archivo que otras herramientas pueden utilizar como lista de entrada. Utilice la opción **-s** para especificar un nombre de archivo. Emailharvester crea archivos XML y

de texto. Proporcione una ruta si lo desea. De lo contrario, los archivos aparecerán en la carpeta **\user\share\emailharvester** . Inspeccione el contenido de los archivos.



Parte 2: Vea los metadatos del archivo.

Los metadatos de archivos pueden proporcionar a los piratas informáticos información sobre las organizaciones y el personal. Por ejemplo, los metadatos dentro de un archivo de imagen pueden revelar el dispositivo que se utilizó para crear la imagen. Esto puede revelar información que puede utilizarse para determinar si el dispositivo es potencialmente vulnerable. Algunos archivos tienen metadatos que consisten en comentarios, el nombre del autor, los nombres de usuario, el sistema operativo o la ubicación en la que se creó el archivo. Los metadatos varían según el tipo de archivo y el dispositivo en el que se crearon. Los hackers pueden utilizar esta información para armar un medio de ataque.

En general, los metadatos de los archivos que se publican en la Internet pública deben eliminarse o al menos analizarse. Puede utilizar ExifTool, entre otros, para eliminar o editar etiquetas de archivos individuales o un directorio de archivos.

ExifTool viene en una versión GUI que está disponible para Windows, MacOS y Linux.

Paso 1: Instale ExifTool.

a. En Firefox, haga clic en el acceso directo de **Kali Tools** o vaya a https://www.kali.org/tools.

b. Seleccione **List all tools** según sea necesario. Busque la entrada **libimage-exiftool-perl**.

c. Siga estas instrucciones de instalación.

d. ExifTool hace referencia a los atributos de metarchivo como etiquetas. Utilice la opción **-list** para ver todas las etiquetas que ExifTool puede procesar.

e. Emita el comando **exiftool -listf** para revisar los tipos de archivo que ExifTool puede analizar.

f. Analice una foto o una imagen de su computadora para ver toda la información que se puede obtener con la herramienta exiftool