Universidad Autónoma de Baja California

Facultad de Ciencias Químicas e Ingeniería



**Taller de Sistema Operativo UNIX**

**EDITOR VI**

Docente: Dra. Pérez Ornelas Felicitas

Alumno: Gómez Cárdenas Emmanuel Alberto

Matrícula: 1261509

**ARTICULO**

El investigador de seguridad [Armin Razmjou](https://twitter.com/rawsec) ha descubierto una grave vulnerabilidad en los conocidos editores de texto presentes en la mayoría de distribuciones Linux: Vim y Neovim.

La vulnerabilidad [CVE-2019-12735](https://nvd.nist.gov/vuln/detail/CVE-2019-12735) tiene una puntuación alta puesto que permite a un atacante ejecutar comandos en el sistema operativo de forma remota y tomar control del mismo. De hecho, utilizando un comando es posible saltarse la protección del *sandbox* de Vim.

Razmjou publicó dos pruebas de concepto en su página de GitHub. Una de ellas ofrece un ejemplo de un ataque en la vida real en la que el atacante logra ejecutar un reverse Shell inmediatamente que el usuario abre el archivo, es decir, el atacante logra ejecutar su código para tomar control de la máquina y además establece una conexión.

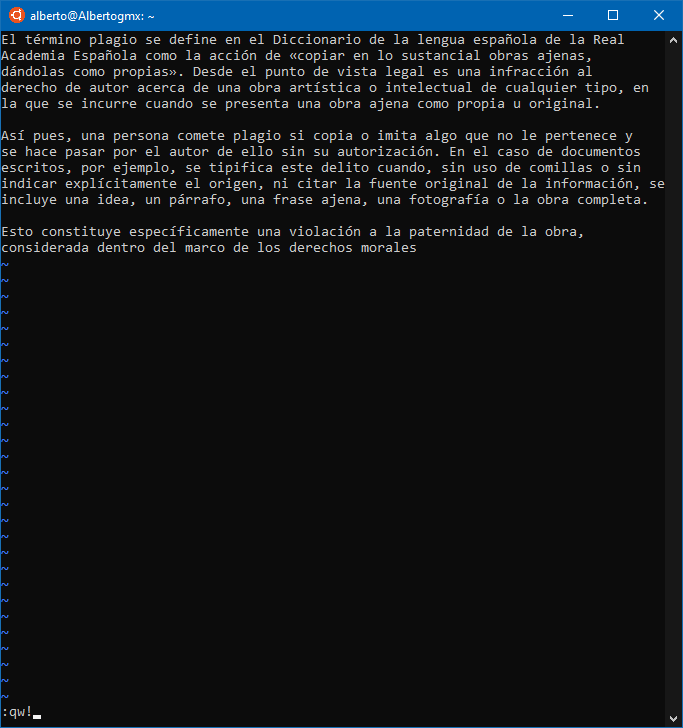
**ACTIVIDADES A REALIZAR**

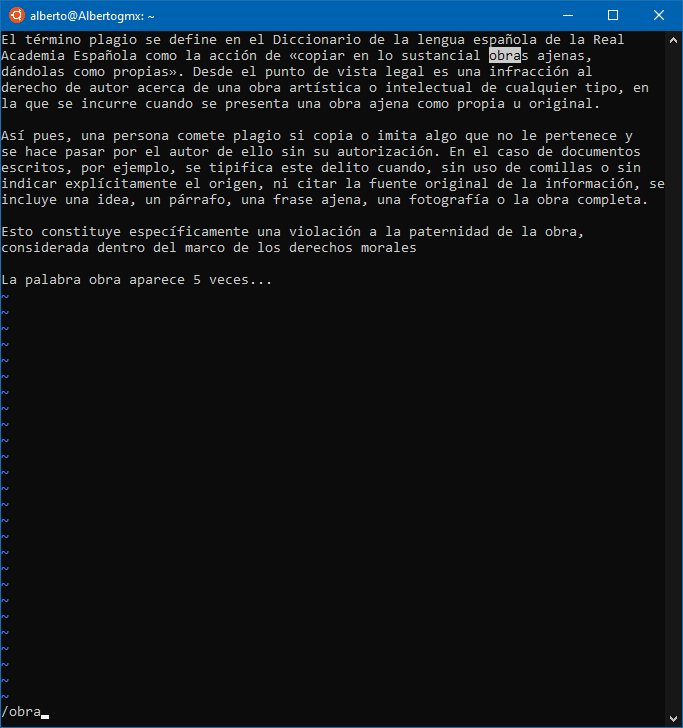
**1. Integrar el siguiente texto en un archivo usando el editor de texto vi (también puede ser vim).**

**El término plagio se define en el Diccionario de la lengua española de la Real Academia Española como la acción de «copiar en lo sustancial obras ajenas, dándolas como propias». Desde el punto de vista legal es una infracción al derecho de autor acerca de una obra artística o intelectual de cualquier tipo, en la que se incurre cuando se presenta una obra ajena como propia u original.**

**Así pues, una persona comete plagio si copia o imita algo que no le pertenece y se hace pasar por el autor de ello sin su autorización. En el caso de documentos escritos, por ejemplo, se tipifica este delito cuando, sin uso de comillas o sin indicar explícitamente el origen, ni citar la fuente original de la información, se incluye una idea, un párrafo, una frase ajena, una fotografía o la obra completa.**

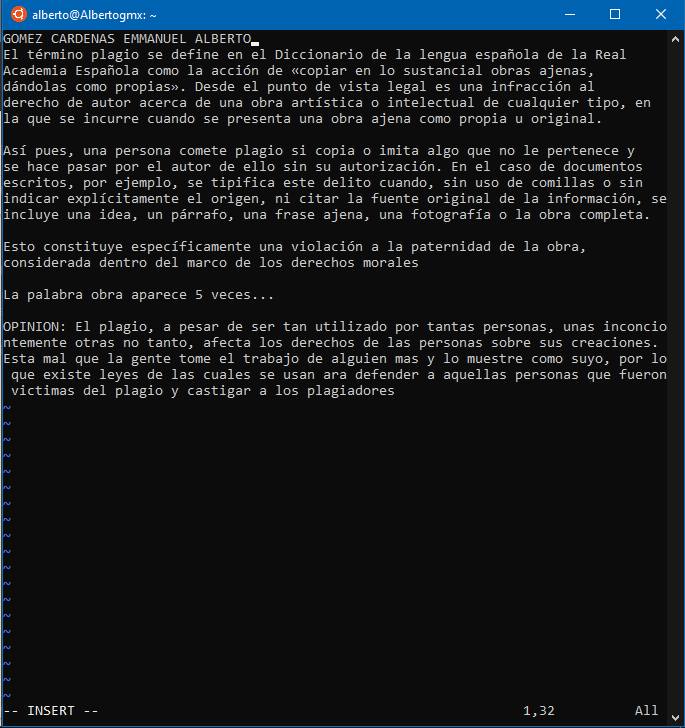
**Esto constituye específicamente una violación a la paternidad de la obra, considerada dentro del marco de los derechos morales.**

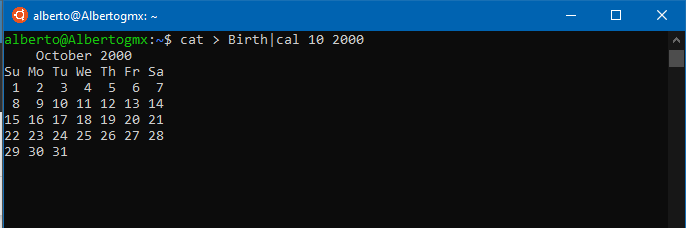
**2. Guardar y salir.** ****

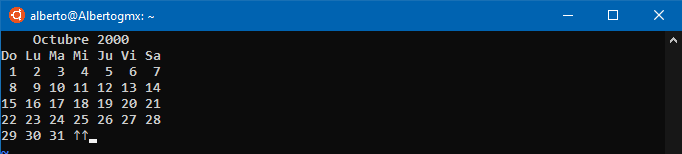
**3. Encuentre el número de veces que se repite la palabra obra (Use el comando de búsqueda de vi para encontrar la palabra y lleve la cuenta manualmente) en el archivo plagio.**

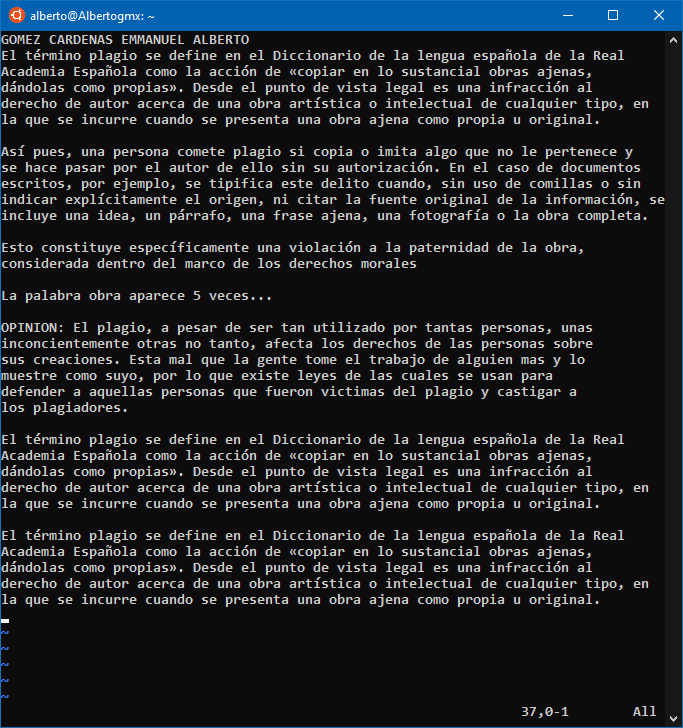
**4. Escriba al inicio su nombre en mayúsculas, en el archivo plagio.**

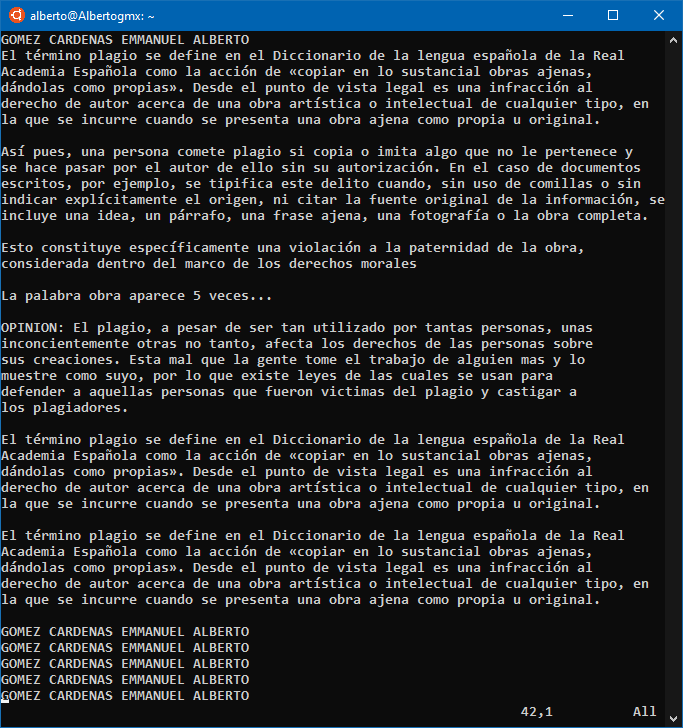
**5. Escriba al final su opinión acerca del plagio, en el archivo plagio.**

****

**6. Utilizando el comando cal y redireccionamiento directo genere un archivo que contenga el calendario del año en que nació, nombre del archivo opcional.** ****

**7. Usando vi, edite el archivo anterior, cambie el calendario al español (en forma manual) y marque el día de su nacimiento.** ****

**8. Copie 2 veces el primer párrafo del archivo plagio, y péguelo al final del texto.** ****

**9. Copie su nombre del archivo plagio 5 veces y péguelo al final del texto.** ****

**10.Cambie a mayúsculas la palabra plagio del archivo plagio.**

**Conclusiones**

El editor VI a pesar de ser tan complejo para aquellas para los primerizos, brinda una recompensa para quienes lo dominan, ya que las funciones te pueden ayudar a mejorar tu rendimiento (esto mismo dicho por los usuarios del editor), ,en cuanto a la noticia, es muy importante darse cuenta de este tipo de vulnerabilidades, debido a que si llega a ser descubierta por alguien malicioso nunca se sabe que tanto podría afectarnos por el simple hecho de abrir un archivo de texto.

**Referencias**

González, G. (2019). Una vulnerabilidad en Vim permite hackear Linux con simplemente abrir un archivo en el editor. Retrieved 20 October 2019, from https://www.genbeta.com/seguridad/vulnerabilidad-vim-permite-hackear-linux-simplemente-abrir-archivo-editor