Ciberseguridad con Inteligencia Artificial

Dr. Vitali Herrera Semenets – CENATAV, La Habana, Cuba (vherrera@cenatav.co.cu)
MSc. Felipe Antonio Trujillo Fernández – IBERO, Ciudad de México, México (felipe.trujillo@ibero.mx)
MSc. Joshua Ismael Haase Hernández– IBERO, Ciudad de México, México (joshua.haase@ibero.mx)
Dr. Lázaro Bustio Martínez – IBERO, Ciudad de México, México (lazaro.bustio@ibero.mx)
Coordinación de Ciencia de Datos - Departamento de Estudios en Ingeniería para la Innovación – Ibero
Primavera 2024

Sesión 1

1. Introducción

En el mundo digital actual, las contraseñas juegan un papel fundamental en la protección de datos y sistemas informáticos. Son la primera línea de defensa contra el acceso no autorizado y, por lo tanto, es crucial que sean sólidas y seguras. Generar contraseñas robustas, conforme a los estándares de seguridad actuales, es esencial para prevenir ataques cibernéticos y salvaguardar la integridad de nuestra información confidencial.

Sin embargo, la seguridad de las contraseñas va más allá de su complejidad. También es crucial mantenerlas en secreto y no compartirlas sin control. La divulgación inadvertida de contraseñas puede abrir la puerta a intrusiones maliciosas y comprometer la seguridad de nuestras cuentas y sistemas.

Además, en el oscuro mundo de la Deep Web y la Dark Net, se encuentran disponibles millones de contraseñas filtradas de brechas de seguridad en diversas plataformas. Estas filtraciones representan un riesgo significativo para la seguridad cibernética, ya que los ciberdelincuentes pueden utilizarlas para llevar a cabo actividades ilícitas como el robo de identidad, el fraude financiero y el acceso no autorizado a sistemas sensibles.

En esta actividad práctica, se explorará cómo aplicar técnicas de Aprendizaje Automatizado para evaluar la fortaleza de las contraseñas y mitigar los riesgos asociados con su uso en un entorno digital cada vez más complejo y vulnerable.

2. Objetivo

Aplicar técnicas de Aprendizaje Automatizado para evaluar la fortaleza de las contraseñas.

3. Indicaciones

a) Obtener los agrupamientos de contraseñas:

- De la web del taller, descargar el dataset "*rockyou.csv*"[1] que contiene un resumen de contraseñas filtradas en la Dark Web.
  El dataset "*rockyou*" comprende 14 millones de contraseñas filtradas de la brecha de seguridad de RockYou Inc. en 2009. Utilizado extensamente en investigación de ciberseguridad, revela patrones comunes de elección de contraseñas, desde simples palabras hasta combinaciones alfanuméricas. Aunque valioso para evaluar la fortaleza de las contraseñas y desarrollar estrategias de seguridad, su uso plantea preocupaciones éticas debido a su origen ilegal. Requiere un enfoque ético y legal en su análisis y aplicación, asegurando la privacidad y el respeto por los derechos de los usuarios cuyos datos están involucrados en la brecha de seguridad.
  Para este ejercicio se usará una versión de "*rockyou*" que contiene todas sus contraseñas, pero se agregaron algunas columnas extras. De esta manera, el dataset "*rockyou.csv*" tiene 14,344,391 contraseñas, y por cada contraseña hay 3 columnas, que se explican a continuación:
  - `password`: texto de la contraseña.
  - `entropy`: valor de entropía de la contraseña[2].
  - `strength`: valor de la fortaleza de la contraseña indicado entre 0 y 1 (inclusive), donde 0 es extremadamente débil y 1 es extremadamente fuerte.
  - `label`: etiqueta que indica si la contraseña es fuerte ("`strong`") o débil ("`weak`").
- Obtenga un resumen estadístico de las contraseñas en el dataset:
  i. Determine la longitud mínima, máxima y media de las contraseñas filtradas. ¿Cuántas contraseñas comparten esa longitud?

[1] https://wiki.skullsecurity.org/index.php/Passwords

[2] La entropía de una contraseña es una medida de la cantidad de incertidumbre o aleatoriedad presente en la contraseña. Se calcula considerando la longitud de la contraseña y la diversidad de caracteres utilizados. Cuanto mayor sea la entropía, más difícil será para un atacante adivinar la contraseña mediante fuerza bruta o métodos similares.

ii. ¿Cuál es el conjunto de caracteres usados en cada uno de los grupos de contraseñas del inciso anterior?
iii. Encuentre las 10 contraseñas más comunes y determine su frecuencia de aparición. Analice las contraseñas encontradas de acuerdo con las indicaciones de los incisos anteriores.

- Aplica un algoritmo de agrupamiento (por ejemplo, KMeans) para agrupar las contraseñas.
  i. Visualiza los grupos obtenidos.
  ii. Entender la naturaleza de los grupos:
    1. Analiza las características de los grupos obtenidos.
    2. Identifica patrones comunes en cada grupo, como longitud, uso de caracteres especiales, etc.
- Modifica el número de grupos a obtener y analiza los nuevos resultados.

b) Entrenar un modelo de clasificación:
- Divide el conjunto de datos en conjuntos de entrenamiento y prueba.
- Selecciona un algoritmo de clasificación adecuado (por ejemplo, SVM) y entrénalo utilizando el conjunto de entrenamiento.
- Evalúa el rendimiento del modelo utilizando el conjunto de prueba.

c) Evaluación de la fortaleza de una contraseña:
- Una vez entrenado el modelo, utiliza la información obtenida para evaluar la fortaleza de una contraseña dada.
- Proporciona una métrica de seguridad basada en la predicción del modelo.

d) Indica las conclusiones a las que has podido arribar sobre la importancia de crear contraseñas sólidas.