Ejercicio#4: El laboratorio de ciberseguridad de una empresa necesita analizar los paquetes de red enviados entre el departamento de recursos humanos y el departamento de ventas aplicando un modelo de reconocimiento de patrones para identificar posibles anomalías de seguridad. Describa con palabras y diagramas que solución propone y porque mediante el uso del lenguaje python. Tomar en cuenta factores como rendimiento y tiempo de desarrollo en la propuesta.

Propuesta de solución utilizando el lenguaje Python

Para analizar los paquetes de red entre los departamentos de Recursos Humanos y Ventas aplicando considero que es necesario aplicar un modelo de reconocimiento de patrones con el objetivo de identificar posibles anomalías de seguridad.

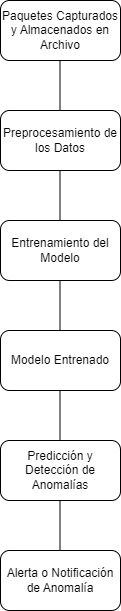
Para abordar este problema, propongo utilizar la biblioteca Scapy en Python. Scapy es una herramienta de manipulación y análisis de paquetes de red que nos permitirá capturar y analizar los paquetes de red enviados entre los departamentos.

Investigando un poco sobre el tema encontré que el primer paso sería capturar los paquetes de red que se intercambian entre los departamentos de Recursos Humanos y Ventas. Podemos hacer esto utilizando Scapy para sniffear y capturar los paquetes en tiempo real. Luego, almacenaríamos estos paquetes capturados en un archivo para su posterior análisis.



Una vez que tenemos los paquetes capturados, podemos proceder al análisis mediante el uso de técnicas de reconocimiento de patrones. Podemos aplicar algoritmos de aprendizaje automático (machine learning) para entrenar un modelo utilizando un conjunto de datos previamente etiquetados. Estos datos etiquetados contendrían tanto tráfico normal como tráfico anómalo.

Podemos utilizar bibliotecas populares de machine learning en Python, como Scikit-learn o TensorFlow, para entrenar y evaluar el modelo. Estas bibliotecas proporcionan una amplia gama de algoritmos de aprendizaje automático y herramientas para el procesamiento de datos.



Una vez que el modelo está entrenado, podemos utilizarlo para realizar predicciones sobre los nuevos paquetes capturados y determinar si contienen anomalías de seguridad. Si el modelo detecta una anomalía, se puede generar una alerta o notificación para que el equipo de ciberseguridad pueda tomar las medidas necesarias.

En cuanto al rendimiento y tiempo de desarrollo, Python es un lenguaje muy adecuado para este tipo de tareas. Es conocido por su legibilidad y facilidad de uso, lo que agiliza el proceso de desarrollo. Además, Python cuenta con una amplia variedad de bibliotecas y herramientas específicas para el análisis de datos y el aprendizaje automático, lo que nos permite aprovechar el trabajo ya realizado por la comunidad y acelerar el desarrollo de la solución.

En resumen, la solución propuesta consiste en utilizar Python y la biblioteca Scapy para capturar y analizar los paquetes de red entre los departamentos de Recursos Humanos y Ventas. Luego, aplicamos técnicas de reconocimiento de patrones utilizando bibliotecas de machine learning en Python para identificar posibles anomalías de seguridad. Esta solución aprovecha la facilidad de uso de herramientas disponibles en Python, lo que nos permite obtener un rendimiento óptimo y un tiempo de desarrollo eficiente.