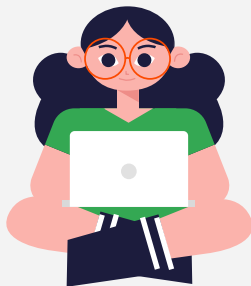


Proyecto



Detección de patrones maliciosos dentro de la red

Start!



¿Cómo saber si me espían a través del wifi?



M

T

W

T

F



Me da miedo que me roben mis contraseñas




M

T

W

T

F



Algunos usuarios son precavidos y se cuestionan sobre la integridad de su información. Mientras otros, asumen que sus datos serán protegidos mientras el uso de la red. **¿Cómo podemos asegurar la seguridad del usuario?**

Objetivo



1

Entrenar un modelo para que detecte **patrones** dentro de la red haciendo uso de la **actividad** (logs) registrados en la nube y así identificar posibles ataques. El propósito es **mantener segura la información de los usuarios conectados** a la red, **alertar** a los administradores en caso de encontrar una actividad sospechosa y **bloquear** al usuario detectado como malicioso.

2

3

4

🔍 Preguntas clave



¿Qué variables son las más importantes al momento de detectar a un intruso dentro de la red?



¿Qué servicios o recursos de la información son más propensos a ser más accedidos durante un ataque?



¿Será prudente tener tres modelos diferentes para poder reducir los errores de falso negativo?

M

T

W

T

F



Investigaciones previas

1. **Android malware detection using network traffic based on sequential deep learning models**

Debido a que las capacidades de un smartphone son cada vez más, cada día hay más usuarios preocupados por la seguridad y privacidad de sus datos. Este artículo habla sobre la detección de anomalías mediante la información básica del tráfico generado, el momento, el tipo de conexión y el tipo de contenido.

2. **Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things**

Este paper presenta el análisis y enfoque que se puede dar con respecto a los modelos de Machine Learning para prevenir ciberataques. Se detalla cómo el campo es enorme, explica sobre el internet de las cosas y todos los riesgos a los que está expuesto el usuario tomando en cuenta la posición del programador.



Investigaciones previas

3. **Detection of Man In The Middle Attacks in Wi-Fi networks by IP Spoofing**

Este paper explica cómo se puede identificar un man in the middle haciendo uso de un segundo router y comparando los tiempos de llegada del cliente hacia el router 1 y router 2. Explicando que si el tiempo de llegada del router 1 es mayor al del router 2, es porque hay alguien en medio robando la información del usuario.

4. **Machine Learning aplicado en Sistemas de Detección de Intrusos**

En este paper se presenta cómo es que se utilizan los Sistemas de Detección de Intrusos (SDI) para detectar a los intrusos en una red con base en logs. Menciona cómo es que estos sistemas se mantienen mediante configuraciones estáticas y el administrador debe de velar por la actualización de las mismas para que no se vea comprometida la información valiosa.

Recolección de datos inicial



1

- Recolección del dataset inicial
- Explicación del dataset inicial
- Limpieza de datos

Veamos el código



2

3

4

Referencias Bibliográficas



1

Anand, Gokul & Prathiba, Sahaya Beni & Gunasekaran, & Ponmani,. (2018). Detection of Man In The Middle Attacks in Wi-Fi networks by IP Spoofing. 319-322. 10.1109/ICoAC44903.2018.8939063.

2

Fallah, S, Bidgoly, AJ. (2022) *Android malware detection using network traffic based on sequential deep learning models*. Softw Pract Exper. 52(9): 1987– 2004. doi:10.1002/spe.3112

3

M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan and R. Jain. (Aug. 2019). *Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things*. IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6822-6834., doi: 10.1109/JIOT.2019.2912022.

4

I. Peluffo, M. Capobianco & J. Echaiz. (2014). *Machine Learning aplicado en Sistemas de Detección de Intrusos*.