Asignatura: Inglés II- Lic. en Sistemas

Segundo Parcial

Nombre y Apellido: Nahuel Quiñones nota 5

Mail: qsnahuel@gmail.com

Entreguen el texto en formato de Word. El parcial puede ser anulado en los siguientes casos: Si se utiliza traductor online. Si se entrega fuera de las 2 horas reloj (hay una tolerancia mínima de 10') Si dos o más alumnos tienen la misma respuesta. Si las respuestas teóricas están copiadas del apunte.

"Conceptualisation of cyberattack prediction with deep learning."

1-Lean y observen el Abstract, luego seleccionen la respuesta que consideren correcta:

1.a La estructura del Abstract es:

A- una estructura formal compuesta por: introducción, finalidad de la investigación y discusión.
B- una estructura formal compuesta por: Introducción, método y resultado
C- una estructura informal.

1.b La cantidad de palabras en un abstract es de:

A- 200 a 500.

B- 300 a 800

C-100 a 800

1.c. El tiempo verbal de este abstract es:

A- Pasado

B- Presente

C-Voz Pasiva. X

1.d. El Abstract esta escrito:

A- Primera persona singular

B- Tercera persona singular.

C-Primera persona del Plural.

2- Observen las siguientes afirmaciones respecto del abstract y digan si son verdaderas o falsas:

A- El en abstract hay ejemplos de sinonimia. Verdadero
B- En el abstract hay ejemplos de antonimia. Falso.
C- En el abstract hay ejemplos de elipsis. Verdadero
D- En el abstract hay ejemplos de referencia. Verdadero
E- En el abstract hay ejemplos de lexicalización. Verdadero
F- En el abstract hay ejemplos de relaciones logicas. Verdadero
G- Las "Keywords" son un campo semántico. Verdadero

3- Busquen en el abstract un ejemplo de cada una de las oraciones que respondieron como verdaderas. Redacten los ejemplos en inglés y su traducción al español.

A-: "*benign and malicious network packets*" y "*benign and malign traffic*". "paquetes de red benignos y malignos" "tráfico benigno y maligno"

C- . "*Though a plethora of extant approaches, models and algorithms…*" "Aunque una abundancia de enfoques, modelos y algoritmos… "se usa para introducir rápidamente un tema, sin profundizar en ellos.

D- .
"*divulging large amounts of information, which can be used for targeted attacks…*" "Which" referencia anaforicamente a "information".

E- . "*Furthermore, the deep learning architecture was co-opted into a new model using rectified linear units (ReLU) as the activation function in the hidden layers of a deep feed forward neural network. Our approach achieves a greedy layer-by-layer learning process that best represents the features useful for predicting cyberattacks in a dataset of benign and malign traffic. The underlying algorithm of the model also performs feature selection, dimensionality reduction, and clustering at the initial stage, to generate a set of input vectors called hyper-features. The model is evaluated using…*" "The model" Es utilizado para lexicalizar los párrafos anteriores.

F- "*New paradigms add more concerns*" "Add" funciona como conector lógico de adición

G- Keywords: Cyberattacks, Prediction, Deep learning, Python, Dimensionality reduction.

4- Observen la palabra "which" en la siguiente oración y respondan:

New paradigms add more concerns with big data collected through device sensors divulging large amounts of information, which can be used for targeted attacks.

¿Qué tipo de palabra es? Es un pronombre relativo impersonal.

¿Cuál es su referente? information

¿Por qué se utiliza en esta estructura? Para relacionar esta oración con la anterior y referirse al elemento previamente mencionado, de esta forma, usa menos palabras y le da cohesión al texto. ok

5- Observen la traducción que realiza el traductor de google del primer párrafo y hagan las modificaciones necesarias para que el texto que se presenta quede bien cohesionado en español. Escriban el texto modificado debajo del cuadro.

Introduccion.

La expansión en el panorama de los ataques ha afectado a gran cantidad de recursos en el ciberespacio. Según Sharafaldin et al. (2018a) y Sharafaldin et al.(2018b), ataques que involucran Botnets, Bruteforce, SQLInyección, Denegación de servicio (DoS), Infiltración, Heartbleed y Denegación de servicio distribuida (DDoS) son teniendo un tremendo efecto adverso en la seguridad detopologias de red. Otros ataques en evolución incluyenanálisis, puerta trasera, exploits, fuzzers, genérico, reconocimiento, shellcode y formularios (Moustafa y Slay2016; Janarthanan y Zargari 2017). Similar,Tobiyama y col. (2016) y Pai et al. (2017) coinciden en quelos usuarios malignos están desarrollando nuevas técnicas que soncapaz de evadir las defensas de la red mientras comprometela estructura interna de las redes. La accesibilidad aBig Data también agrega más preocupaciones a la seguridad dedatos y otros activos digitales. Aunque las investigaciones recientes se han inclinado hacia el modelado de la predicción de ciberataques, se ha vuelto cada vez más difícilIdentificar un enfoque único que resuelva el problema deciberataques en los últimos tiempos.

La mayoría de los enfoques en la literatura se basan en algoritmos específicos de tareas, por lo que requieren la necesidad de un enfoque que se base más en el aprendizaje de la representación.Es decir, un enfoque que puede aprender diferentes ataques clases de datos brutos en lugar de depender de tareas preprogramadas.

Texto corregido:

Introducción.

La expansión en el panorama de los ataques ha afectado a gran cantidad de recursos en el ciberespacio. Según Sharafaldin et al. (2018a) y Sharafaldin et al. (2018b), los ataques que involucran Botnets, Bruteforce, SQLInyección, Denegación de servicio (DoS), Infiltración, Heartbleed y Denegación de servicio distribuida (DDoS) están teniendo un tremendo efecto adverso en la seguridad de topologías de red. -Otros ataques en evolución incluyen "análisis", "puerta trasera", exploits, fuzzers, "genérico", "reconocimiento", shellcode y "formularios" (Moustafa y Slay 2016; Janarthanan y Zargari 2017)-.

Al mismo tiempo, Tobiyama y col. (2016) y Pai et al. (2017) coinciden en que los usuarios malignos están desarrollando nuevas técnicas, las cuales son capaces de evadir las defensas de la red mientras comprometen su estructura interna. La accesibilidad a Big Data también agrega más preocupaciones a esta problemática. Aunque las investigaciones recientes se han inclinado hacia el modelado de la predicción de ciberataques, se ha vuelto cada vez más difícil Identificar un enfoque único que resuelva este problema en los últimos tiempos.

La mayoría de estos enfoques en la literatura se apoyan en algoritmos específicos de tareas, los cuales necesitan de una orientación basada en el aprendizaje de la representación. Es decir, que puede aprender diferentes ataques clases de datos brutos en lugar de depender de tareas preprogramadas.

6- Finalmente, comente cuales son los principales errores que comete el traductor.

La falta del uso de referencias, no hace uso de la lexicalización ni de la elipsis. También falla en la puntuación. incompleto