Inteligencia Artificial, Machine Learning, Deep Learning aplicados a la Ciberseguridad

Clara Flores Siñani
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
clara.flores.s@gmail.com

***Resumen*—En la actualidad los Ciberataques son las amenazas que hay que combatir, los riesgos de la ciberdelincuencia son una realidad palpable y medible en cifras. La Seguridad Informática se encuentra en constante evolución y dinamismo, hoy en día la aplicación de técnicas de Inteligencia Artificial se convierte en una práctica indispensable en el tratamiento y detección de amenazas a que se encuentran expuestas las organizaciones. El desarrollo de las tecnologías de la información y las comunicaciones requiere de mecanismos de ciberseguridad que garanticen la confidencialidad, integridad y disponibilidad de la información, y del desarrollo de habilidades para detectar y controlar oportunamente las nuevas amenazas.**

Palabras clave—Ciberseguridad, Machine Learning, seguridad, ciberataques, ciberdelincuentes, SQL Injection

I. INTRODUCCIÓN

Los ciberataques son un gran inconveniente para las organizaciones, entre las razones más importante: pérdidas económicas, daño a su reputación, robo de información, con las nuevas tecnologías los ciberdelincuentes también van actualizándose y buscando cuales usar a su favor.

Los ataques cibernéticos o ciberataques aprovechan las vulnerabilidades, ya estén asociadas al software, a los dispositivos informáticos o a las personas que los administran y utilizan. Con el aumento de la complejidad de los sitios web y el rápido desarrollo de aplicaciones, aumenta la posibilidad de sufrir ataques. Mientras tanto, los piratas informáticos y ciber mercenarios crean, distribuyen y utilizan sofisticadas herramientas de exploit y malware para robar o destruir datos empresariales fundamentales, comprometer sitios web e interrumpir estructuras operativas.

Las empresas, en particular las que han sufrido los efectos de los ciberataques, han reforzado los controles de seguridad perimetrales, como los firewalls y los sistemas de detección de intrusiones. Por desgracia, los métodos de seguridad de centros de datos tradicionales como estos no son suficientes para proteger a las empresas frente a amenazas cibernéticas distribuidas a gran escala o ataques furtivos en el nivel de aplicación [1].

II. MÉTODOS

A. Ciberseguridad según ISACA

ISACA es el acrónimo de Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información), una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información. De acuerdo con la asociación, puede entenderse como:

"Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".

La norma ISO 27001 define activo de información como los conocimientos o datos que tienen valor para una organización, mientras que los sistemas de información comprenden a las aplicaciones, servicios, activos de tecnologías de información u otros componentes que permiten el manejo de la misma.

Por lo tanto, la ciberseguridad tiene como foco la protección de la información digital que se encuentra en los sistemas interconectados. En consecuencia, está comprendida dentro de la seguridad de la información.

B. Seguridad Informática

La seguridad informática es la disciplina que se Ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos [1][2]. Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

La seguridad informática consiste en asegurar en que los recursos del sistema de información de una organización se utilizan de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización [3].

C. Incidente de Seguridad Informática

Los diferentes ataques que sufren los sistemas conectados a Internet son conocidos como incidentes de seguridad informática. Éstos amenazan el buen funcionamiento de cualquier organización y violan implícita o explícitamente las políticas de seguridad [5].

Para referenciar este artículo (IEEE):

[N] C. Flores, «Inteligencia Artificial, Machine Learning, Deep Learning aplicados a la Ciberseguridad», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 7, pp. 11-13, 2020.

Los incidentes pueden ser causados por intrusos informáticos, extorsionadores, espías industriales, usuarios del sistema, ex empleados o jóvenes queriendo probar sus técnicas, con el objetivo de robar información, fraudes financieros, daño a la imagen, modificación de archivos, inhabilitar los servicios críticos, destrucción de sistemas informáticos o sabotaje corporativo.

D. Ranking de los 10 Riesgos de Seguridad de OWASP

Para concientizar OWASP muestra un ranking con los principales riesgos de seguridad [5].

1. Injection
2. Broken Authentication
3. Sensitive data exposure
4. XML External Entities (XXE)
5. Broken Access control
6. Security misconfigurations
7. Cross Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with known vulnerabilities
10. Insufficient logging and monitoring

E. Tipos de Ciberataques

- Malware

Malware se refiere a varias formas de software dañino, como virus y ransomware. Una vez que entra en el ordenador, puede causar todo tipo de estragos, desde tomar el control de la máquina y monitorear las acciones y pulsaciones de teclas, hasta enviar silenciosamente todo tipo de datos confidenciales a la base de origen del atacante [2].

Es uno de los más conocidos para el público general y se presenta de formas tan habituales como una alerta de antivirus en la pantalla o tras hacer clic erróneamente en un archivo adjunto de correo electrónico malicioso. Es muy efectivo y los atacantes suelen utilizarlo para entrar en los ordenadores de usuarios particulares y en oficinas [3].

Aunque existen varios métodos para introducir este ataque en un ordenador, en algún momento requiere que el usuario realice una acción para instalar el malware. [2].

- Phishing

También se conoce como suplantación de identidad, ya que suele ser la principal vía que utilizan. Para combatir este tipo de ataques, es esencial comprender la importancia de verificar los remitentes de correo electrónico y los archivos adjuntos y enlaces [9].

Los atacantes saben que lo más probable es que un usuario no abra un archivo adjunto al azar o haga clic en un enlace de cualquier correo electrónico. Por ello, a menudo simulan ser alguien o alguna otra cosa para conseguir que se realice la acción deseada. Como dependen de la curiosidad y los impulsos humanos, estos ataques son difíciles de detener.

- Ataque de inyección SQL

El SQL es un lenguaje de programación de consulta estructurado y utilizado para comunicarse con las bases de datos. Muchos de los servidores que almacenan información crítica para sitios web y servicios lo usan [2].

Un ataque de inyección SQL apunta específicamente a este tipo de servidor, utilizando código malicioso para extraer su información. Esto es especialmente problemático si el almacenamiento incluye datos privados de clientes, como números de tarjetas de crédito, nombres de usuario y contraseñas.

- Cross-Site Scripting (XSS)

A diferencia del ataque a SQL, este tipo persigue al usuario y no al servidor. Implica la inyección de código malicioso en un sitio web, que se ejecuta en el navegador del usuario cuando este accede al mismo.

Una de las formas más comunes para implementar este tipo de ataque entre sitios es mediante la inyección de código malicioso en un comentario o un script que se puede ejecutar automáticamente.

Los ataques de secuencias de comandos en sitios cruzados pueden dañar significativamente la reputación de un sitio web al poner en riesgo la información de los usuarios sin ninguna indicación de que haya ocurrido algo malicioso [3].

- Denegación de servicio (DOS)

Consiste en saturar de tráfico un sitio web, sobrecargando su servidor para que le sea imposible publicar su contenido a los visitantes. Aunque esto puede ocurrir porque el enlace de una noticia masiva se haya roto, a menudo es provocado con fines maliciosos [2].

En algunos casos, estos ataques DoS son realizados por muchos ordenadores al mismo tiempo. Son muy difíciles de superar debido a que el atacante aparece simultáneamente desde diferentes direcciones IP en todo el mundo, lo que dificulta aún más la determinación del origen [10].

III. RESULTADOS

A. Machine Learning para el Pentesting: La Importancia de la IA en el ámbito de la Ciberseguridad

Muchas empresas utilizan herramientas para analizar la seguridad de sus productos, una de estas herramientas son las GANS (Generative Adversarial Networks) y con ellas se puede detectar los fallos que hay en un modelo de Machine Learning. Además, se pueden utilizar para entrenar determinados modelos y hacerlos más robustos. Las GANS son algoritmos de inteligencia artificial diseñados para llevar a cabo aprendizaje automático no supervisado, están compuestos por un sistema de redes neuronales que compiten entre sí [4].

B. DEEP-PWNING

Es un pequeño framework escrito en Tensorflow que sirve para experimentar con modelos de machine learning con el fin de evaluar su nivel de robustez frente a un adversario motivado. En la actualidad Deep-pwning no ha alcanzado su máximo desarrollo, se trata de un framework con el que experimentar y cuyos conocimientos se expanden paulatinamente abriendo así la posibilidad de que en un futuro pueda convertirse en una herramienta para realizar test de penetración y estudios estadísticos sobre algunos modelos machine learning.

C. ADVERSARIAL LIB

Esta librería escrita en Python es open source y al igual que Deep-pwning está diseñada para evaluar la seguridad de los clasificadores machine learning frente a los “adversarial atacks”. Viene con diversas funciones muy potentes [4].

Su uso es tan sencillo como lanzar un script. Soporta un amplio rango de algoritmos de machine learning, los cuales optimiza y reescribe en C++. Además, en caso de necesitar un algoritmo que no se encuentre en la librería, se puede añadir a ésta, convirtiéndola así en una herramienta cada vez más completa [9].

D. THE GAN ZOO

Es una página de referencia en la que se pueden encontrar infinidad de GANS con las que poner a prueba y entrenar modelos de machine learning. The GAN Zoo tiene detrás de sí una gran comunidad de desarrolladores que cada semana añaden nuevos papers a su repositorio en GitHub [4][6].

El machine learning se ha convertido en una poderosa herramienta para los desarrolladores e investigadores en el campo de la seguridad informática. La posibilidad de utilizar una herramienta para llevar a cabo numerosos test de seguridad y penetración ahorra mucho tiempo y esfuerzo a los investigadores permitiéndoles centrarse en otras tareas simultáneamente [7].

E. Deep Learning en Ciberseguridad: la herramienta definitiva

Su gran fortaleza es que aprende a tiempo real y permite desarrollar los nuevos criterios de clasificación sin intervención humana. Por ejemplo, se está aplicando contra el malware y el fraude online. ¿Por qué? Porque los cibercriminales evolucionan rápidamente, generando amenazas capaces de adaptarse a la seguridad de los sistemas. Por consiguiente, Deep Learning es capaz de detectar y clasificar dichas amenazas y ponerlas solución de forma eficiente y veloz [5][8].

No obstante, sus aplicaciones son infinitas, por ejemplo, en el caso de buguroo se utiliza como método de identificación. Lo que les permite reconocer si el usuario es un humano o un bot, si un cibercriminal está intentando suplantar una identidad de usuario, o si un cibercriminal está interactuando con la cuenta de un usuario desde cualquier parte del mundo.

IV. DISCUSIÓN

Su uso permite mantener a los sistemas completamente actualizados. Los viejos modelos de defensa analizan solo aquello que ya se conoce, alejándose de lo que las compañías necesitan. Actualmente, el reto del sector de la ciberseguridad es poder estar preparado para aquello que todavía no se conoce.

Así puede detectar patrones de comportamiento en las redes y predecir ataques futuros a las empresas u organizaciones.

Algunos de los trabajos relacionados a esta temática son la Tesis de Grado de la UMSA de Detección de SQL Injection Basada en Random Forest" elaborado por Efrain Rojas.

REFERENCIAS

[1] «Akamai,» [En línea]. Available: https://www.akamai.com/es/es/resources/cyber-attacks.jsp. [Último acceso: 29 Septiembre 2019].

[2] Cámara Valencia, «Tecnología para los Negocios,» [En línea]. Available: https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-un-ciberataque-y-que-tipos-existen/. [Último acceso: 25 Septiembre 2019].

[3] A. Hern, «The Guardian,» 1 Noviembre 2016. [En línea]. Available: https://www.theguardian.com/technology/2016/nov/01/cyber-attacks-hacking-philip-hammond-state-cybercrime. [Último acceso: 26 Septiembre 2019].

[4] S. S. Azcoitia, «Telefónica,» 9 Enero 2019. [En línea]. Available: https://empresas.blogthinkbig.com/machine-learning-para-el-pentesting-la/. [Último acceso: 26 Septiembre 2019].

[5] Universidad de Alcalá, «Universidad de Alcalá,» [En línea]. Available: https://master-deeplearning.com/camino-deep-learning-ciberseguridad/. [Último acceso: 28 Septiembre 2019].

[6] M. Rouse, «Search Data Center,» [En línea]. Available: http://searchdatacenter.techtarget.com/es/definicion/Inteligencia-artificial-o-AI.

[7] E. Moya, «Deep Learning en ciberseguridad: La herramienta definitiva» 11 12 2017.

[8] 20 Min Tecnología, «20 Min Tecnología,» 15 Enero 2017. [En línea]. Available: http://www.20minutos.es/noticia/2932536/0/inteligencia-artificial-ventajas-riesgos-mundo-maquinas-humanas/.

[9] J. Zambrano, «¿Aprendizaje supervisado o no supervisado? Conoce sus diferencias dentro del machine learning y la automatización inteligente,» Medium, 18 03 2018.

[10] A. Muñoz, Interviewee, Machine learning aplicado a ciberseguridad. [Entrevista]. 23 12 2017.

Breve CV de la autora

Clara Flores Siñani es Licenciada en Informática, titulada de la Carrera de Informática de la Universidad Mayor de San Andrés, La Paz. Trabajó en la Fuerza Aérea Boliviana, la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) y el Registro Único para la Administración Tributaria Municipal (RUAT). Email: clara.flores.s@gmail.com.