Análisis de ejercicios de Ataque y Defensa en Ciberseguridad: Equipo Rojo versus Azul

Analysis about Attack and Defense exercises in Cibersecurity: Read versus Blue Teams

Ponce Almeida Julio Josué[1]*, Montes Vera Jéssica Johana[2], García Vera Manuel Jacinto[3], Zambrano Rendon Aura Dolores[4]

julio.ponce@espam.edu.ec, jessica.montes@espam.edu.ec, manuel.garcia@espam.edu.ec, azambrano@espam.edu.ec

Resumen

La ciberseguridad es un campo crucial en la sociedad tecnológica, pues es necesario que un sistema sea confiable y seguro contra ataques informáticos; sin embargo, ninguno es completamente infalible, ya que pueden llamar la atención de terceros maliciosos, atraídos por la idea de lograr penetrar en la seguridad de la red, accediendo a información sensible para obtener beneficios, como la venta de la información a los mejores postores en mercados negros. En efecto, las empresas y los gobiernos están invirtiendo cada vez más en ciberseguridad, pero aún no han logrado mantenerse al día con los ciberdelincuentes. Por tal motivo, el presente artículo tiene como objetivo presentar una metodología de investigación sobre los ejercicios de ataques y defensas en el área. Se comenzará con una introducción a la ciberseguridad y luego se proporcionarán ejemplos de las modalidades de simulacro de estos ataques. Se discutirá también las herramientas y técnicas que se utilizan en el mundo real para llevar a cabo los crímenes cibernéticos, y que son parte importante de la simulación. A través de la observación de lo estudiado, se ha identificado tres puntos principales de la ciberseguridad: los ataques cibernéticos pueden tener un impacto significativo en la sociedad y la economía, las brechas en la seguridad son una amenaza para todos los sectores, no solo para aquellos que tienen una presencia online y los cibercrímenes son una amenaza para todos los países, no solo para aquellos con una economía más desarrollada.

Palabras clave: Equipo Rojo; Equipo Azul; Ataque; Defensa; Ciberseguridad; Vulnerabilidades

Abstract

Cybersecurity is a crucial field in our technological society, because it is required that a system is trustworthy and secure against informatics attacks; however, no system is infallible, because they can lure the attention of malicious third parties, attracted by the idea of achieving a breakthrough on the system's security, accessing to sensible information to obtain benefits by selling it to the best bidder in black markets, and due to this, companies and governments are investing more and more into cybersecurity to engage into a race against cybercriminals. For this motive, this article will have the objective of presenting an investigation methodology about attack and defense exercises in this area. The article will start with an introduction to cybersecurity, examples of the different modalities of these simulated attacks. It will also be discussed the tools and techniques utilized in the real world to commit the crimes, and that take an important role in attack and defense exercises. Through the observation of the previously detailed data, three main cybersecurity's points were identified: cybernetic attacks can have a significant in society and economy, security breaches are a menace to all sectors, not only for those who as an online presence and cybercrimes are a menace to all countries, not only those with a developed economy.

Keywords: Red Team; Blue Team; Attack; Defense; Cybersecurity; Vulnerabilities

1. Introducción

El espacio virtual o ciberespacio cada día se encuentra más presente y que al igual que con espacios físicos, este requiere de su propia forma de protegerlo, aquí entra el concepto de ciberseguridad el cual se trata de un campo que viene del proceso de protección del ciberespacio de ataques criminales y amenazas y problemas varios los cuales se puede dividir en tres categorías troncales tales como son las amenazas como adversarios del estado, espías, criminales, terroristas; las vulnerabilidades las cuales son puntos débiles en un sistema que pueden permitir que internos maliciosos puedan manipularlo, así como permitir la ejecución de código malicioso dentro del sistema; y, finalmente, los impactos los cuales son consecuencia de un ataque exitoso donde se compromete la integridad, disponibilidad y confidencialidad de un sistema (Fischer, 2016), por nombrar un par de ejemplos.

Debido a la constante evolución de las formas en que se ataca el ciberespacio se han desarrollado y desplegado varias formas para proteger datos que son o se consideran críticos como por ejemplo sofisticados sistemas de monitoreo de contenido, gestores de contraseñas, Firewalls más efectivos, etc. Si bien todas estas mejoras ofrecen un alto nivel de protección que pueden ayudar a combatir estos problemas, pero aun así falta otro componente fundamental, los usuarios quienes, para evitar y prevenir estas amenazas, deben conocer y cumplir con las normativas de seguridad informática de la entidad a quienes pertenecen, todo esto con la finalidad de que se evite la filtración intencional o no de datos valiosos y sensibles (Li et al, 2019). La importancia de estos aspectos es sumamente alta ya que en el año 2014 la vulneración de la seguridad en sistemas de grandes instituciones y los posteriores cibercrímenes cometidos habían provocado un estimado de 575 mil millones de dólares en pérdidas debido a que el objetivo central detrás del porqué se suelen cometer estos crímenes suelen tratarse sobre el robo de dinero, propiedad intelectual, así como datos para su posterior venta o su uso en crímenes relacionados con la extorsión de los usuarios o personas a quienes pertenezca la información (Martin et al, 2017).

Pero la ciberseguridad es más que solo métodos y capacitación de usuarios, sino que intervienen dos aspectos muy importantes, las estrategias de ataque y defensa, donde se vulnera un sistema para buscar sus defectos y se defiende el mismo en caso de que exista un ataque a dicha vulneración, a menudo referidos como Equipo Rojo y Equipo Azul de manera respectiva.

El objetivo del presente artículo es presentar una metodología de investigación sobre los ejercicios de ataques y defensas, cómo funcionan y la importancia de estos equipos dentro de la ciberseguridad mediante una búsqueda y fundamentación bibliográfica.

2. Materiales y Métodos

Para la obtención de la información y así llevar a cabalidad el objetivo del artículo se empleó la metodología bibliográfica, esta forma parte de lo que se conoce como Metodología de la Investigación (Fuentes-Doria et al, 2020), mediante la cual consta de tres fases: definición de la búsqueda, búsqueda bibliográfica, y, análisis y comprensión.

2.1. Definición de la búsqueda

Para el desarrollo de la investigación realizada se necesitó el uso de documentación académica relacionados con “Análisis de ejercicios de Ataque y Defensa en Ciberseguridad: Equipo Rojo versus Azul”, además se realizó una búsqueda exhaustiva de las siguientes palabras clave: Equipo Rojo, Equipo Azul, ataque, defensa, ciberseguridad, vulnerabilidades; con la ayuda de motores de búsqueda especializados en artículos tales como Scholar Google (Google Académico), IEEExplore, Scielo y Dialnet.

2.2. Búsqueda bibliográfica

Mediante el uso de los motores previamente mencionados fue realizada una búsqueda extensiva de información relevante tomando en cuenta que la fecha de publicación de los artículos consultados no exceda en más de cinco años de la fecha de redacción del presente trabajo, esto se realiza por motivos de relevancia, y así se filtra en su mayor parte información que podría llegar a considerarse obsoleta.

Tabla 1 – Campos que se consideraron en la recopilación de información.

Campos	Descripción
Año	Año en el que se aprobó y publicó el artículo científico. Solo se investigaron artículos con al menos de 5 años de antigüedad.
Título	Nombre con el que se identifica el artículo.
Autor(es)	Aquellos que participaron en la elaboración de los artículos investigados.
Ejercicios de Ataque y Defensa	Investigación sobre los ejercicios de ataques y defensas en el área de ciberseguridad: Equipo Rojo versus Azul.

2.3. Análisis y comprensión

Finalmente, en esta fase, se procederá a realizar el análisis de la información recopilada y tomar los aspectos más relevantes de cada trabajo consultado, de esta forma se puede sustentar cada explicación.

Con base a lo anterior, se determinaron que en el campo de la Ciberseguridad, la amenaza de los ciberataques se cierne de manera constante por lo que a manera didáctica se suelen hacer ejercicios de Equipo Rojo contra equipo Azul, atacantes contra defensores, todo esto a modo de entrenamiento o para probar la seguridad de la infraestructura completa del sistema, a menudo esta didáctica se le conoce bajo el nombre de “Ejercicios de Equipo Rojo – Equipo Azul”, un aspecto de alta importancia a considerar antes de llevar a cabalidad los ejercicios es la correcta definición de las entidades que componen los equipos así como la estructura todo esto parar lograr un simulacro con un mínimo de un sistema en cada lado administrado respectivamente por un equipo (A cada sistema extra que se añada este deberá ser supervisado por un nuevo equipo) (Otsby et al, 2019).

Los ejercicios de Ataque y Defensa, son realizados mediante tres modalidades en entornos previamente creados o establecidos donde deben llevar a cabo sus respectivas labores, los cuales son:

Ejercicio de Ciberataque. - Se trata de que el Equipo Rojo deberá de vulnerar un sistema o alcanzar una serie de objetivos (a menudo la obtención de datos importantes y que potencialmente podrían ser de interés de criminales reales) en un marco de tiempo específico.

Ejercicio de Ciberdefensa. - En este ejercicio, el Equipo Azul deberá de investigar y prevenir un ataque cibernético en un tiempo límite.

Ejercicio de Ciberataque y Ciberdefensa. - Ambos equipos se enfrentan de manera concurrente el uno contra el otro de manera completamente activa tratando de vulnerar y defender un sistema respectivamente con el objetivo de simular diferentes escenarios sin el peligro real de perder información, si bien parece que esto podría generar perdedores y ganadores esto es irrelevante ya que el objetivo de este ejercicio es la preparación a conciencia mediante el simulacro (Yamin & Katt, 2019).

3. Resultados y Discusión

A. RESULTADOS DE LA INVESTIGACIÓN

Tras realizar una correcta investigación en base a la metodología presentada anteriormente, este trabajo investigativo y su posterior análisis permitirá llegar a comprender de manera más profunda las entidades importantes que forman parte de las estrategias o ejercicios de simulación dentro del campo de la Ciberseguridad.

1. EQUIPO ROJO: ATACANTES

El Equipo Rojo o Atacantes se trata de un conjunto o grupo de profesionales de la Ciberseguridad en lo que se conoce como una forma de “Hackeo Ético” que tiene como objetivo troncal proveer un “golpe de realidad” al sistema de una institución para demostrar el impacto que puede tener la explotación de vulnerabilidades con tal de informar a los gestores de riesgo de la institución, todo esto mediante el uso de todas las técnicas disponibles para encontrar y aprovecharse de los puntos débiles anteriormente mencionados. Gracias al Equipo Rojo se puede llegar a emular adversarios o criminales en pleno ataque con tal de estudiar el caso con motivos defensivos y preventivos mediante el desafío de la seguridad de la infraestructura de manera táctica, sin embargo, si

este equipo nunca ha sido a prueba no puede afinar y madurar para poder lograr un ataque eficaz al sistema objetivo (Rehberger, 2020).

Usualmente, gracias al uso de estas técnicas o estrategias, el ataque suele desembocar en el robo de credenciales de usuario de alto nivel tales como administradores o usuarios especiales con tal de acceder a información que se considere crítica para simular el objetivo de atacantes con fines verdaderamente maliciosos.

2. EQUIPO AZUL: DEFENSORES

El Equipo Azul o Defensores es un grupo que se encuentra en una posición diametralmente opuesta al del Equipo rojo, al tratarse de que su objetivo primordial es el de proteger un sistema de un ataque (Yamin et al, 2021), esto mediante la documentación del sistema, así como de reforzar el mismo aumentando la seguridad de las credenciales y ayudando a implementar políticas de seguridad más estrictas.
Por lo que se puede establecer que un Equipo Azul, al igual que el Equipo Rojo, es un conjunto de profesionales de la Ciberseguridad, pero enfocados a la protección y refuerzo de un sistema, así como la comunicación de los problemas que surjan, la primera línea de defensa en contra de un ataque, sujetos a las mismas regulaciones tales como:

- Se debe concretar la defensa en un periodo de tiempo dado.
- Seguir un contrato previamente establecido, lo cual permite evitar problemas legales entre el Equipo y la Institución debido al manejo de información sensible.
- Seguir el contexto de la operación de defensa.

3. TÉCNICAS Y HERRAMIENTAS

Contrario a lo que podría parecer, este tipo de equipos se enfocan más en la correcta planeación de sus ataques y defensas, así como el mesurado estudio de los puntos de quiebre a explotar dentro del sistema, a menudo desplegando un amplio arsenal a su disposición con tal de lograr su objetivo, como son:

- Footprinting (Información legalmente disponible para realizar un ataque).
- Fingerprinting (Reconocer el sistema a atacar).
- Phishing (Robo de contraseñas mediante enlaces maliciosos).
- Identificación de posibles contraseñas filtradas de algún usuario o empleado sea o no que siga trabajando en la institución.
- Ingeniería social.
- Nmap (Herramienta para reconocer equipos en una red).
- Social Engineering Toolkit (Conjunto de herramientas para ejercer ingeniería social con todas sus técnicas).
- Metasploit (Programa de administración de exploits que permite aprovechar vulnerabilidades en diversos programas dentro de una maquina conectada a una red).
- Sistemas trampa o Honeypot (Un sistema falso para que los atacantes caigan en él).
- Sistema sandbox (Un sistema aislado para experimentar ataques y formas de evitarlos o paliarlos).

Estos son algunas de las técnicas y herramientas utilizadas por los equipos rojo y azul (Straub, 2020).

Tabla 2. Clasificación de herramientas y técnicas del Equipo Rojo. Fuente: (Diogenes & Ozkaya, 2018)

Herramientas	Técnicas
Nmap	Footprinting
Sqlmap	Fingerprinting
Nikto	Phishing
Social Engineering Toolkit	Smishing
Metasploit	Exploits de día cero
Wireshark	Extorsión
IDA PRO	Puertas traseras
Konboot	Registro remoto
Ophcrack	Robo de credenciales
Nimbostratus	Ataque DDoS

Tabla 3. Clasificación de herramientas y técnicas del Equipo Azul. Fuente: (Diogenes & Ozkaya, 2018)

Herramientas	Técnicas
Elastic Honey	Honeypot
Firejail	Sandbox
Cyphon	Respuesta a incidentes
ASI	Reducción de la superficie de ataque
LANDesk Management Suit	Administración de vulnerabilidades
Microsoft Threat Intelligence Center	Segmentación de la red
Threat Intelligence Exchange	Sistemas de detección de intrusos
Secunia PSI	Sistemas de prevención de intrusos
ArcSight Enterprise Security Manager	Creación de respaldos
Virtual Switch Manager for ARGOS	Aseguramiento del acceso remoto a la red

4. EMPRESAS Y SUS ESTRATEGIAS DE DEFENSA: FORTALEZAS Y DEBILIDADES

A continuación, se detallará el acercamiento de algunas empresas a la ciberseguridad, así como sus fortalezas y debilidades producto de sus estrategias para defender la integridad de sus sistemas de información:

Tabla 4. Empresas y las Fortalezas y Debilidades en su acercamiento a la seguridad de sus sistemas. Fuentes: (Roussel-Tarbouriech et al, 2019), (Smith et al, 2020) y (Zhou & Sun, 2020)

Estrategia de la empresa	**Fortalezas**	**Debilidades**
Huawei: Denominada "Winter-is-coming", prepararse para lo per	Mediante los diferentes recursos y cultura de equipo se permite diferentes estrategias y el desconocimiento de estas entre ambos grupos se adquiere una mayor experiencia tras los ejercicios de ataque y defensa, ofreciendo un sitio en el equipo Azul a los más destacados del equipo Rojo	La alta estima del equipo Rojo dentro de la empresa puede generar problemas de confianza tras cualquier tipo de fallas en su trabajo porqué "Si no puedes derrotar a Huawei (Equipo Azul), has tocado techo"
Microsoft: Motivar a los equipos a modo de que se vean como compañeros de entrenamiento	Gracias una cultura de trabajo basada en el compañerismo se consigue los resultados de la contienda se compartan entre los equipos y se motiva a trabajar en los errores descubiertos, ya sea para arreglarlos o para teorizar lo que pasaría al explotarlos	Si bien la confianza humana es importante, también lo es las herramientas, y muchas de las herramientas utilizadas por los Equipos en Microsoft no permiten la comprensión o explicación de código (lenguaje único de las herramientas) así como permitir la automatización de ciertas acciones críticas en caso de un ataque real
Nintendo: Arreglar los problemas según vayan surgiendo.	A medida que surgen las complicaciones las van arreglando, por lo que se permite un correcto arreglo de cualquier vulnerabilidad con cada actualización de manera pronta y responsable	Debido a los métodos y enfoque tradicionalista de Nintendo, cualquier aspecto vulnerable existente que pase o pueda pasar desapercibida puede provocarles grandes daños a la integridad de su seguridad

B. DISCUSIÓN

Con los datos recabados, se puede observar la importancia de los ejercicios de Ataque y Defensa, no solo como un simulacro de lo que se debería de hacer en caso de un ataque lo cual cumple con el objetivo de los ejercicios, se observó el acercamiento de las compañías a estos conceptos y como les ayuda. Para poner en perspectiva la importancia de los ejercicios de Equipo Rojo contra Equipo Azul, en el caso del Banco Pichincha durante el transcurso del último cuatrimestre del año 2021 sufrió un ataque informático malicioso en el cuál grandes cantidades de información sensible como usuarios y claves de acceso a la banca virtual de una gran cantidad de gente, información de la cual se pidió un rescate (El Universo, 2021), si bien los resultados de este evento no fueron discutidos públicamente más allá de volver a ofrecer sus servicios, este es un aliciente que demuestra la gran importancia que poseen las simulaciones entre atacantes y defensores, se pueden encontrar vulnerabilidades antes que los criminales que solo buscan explotar y robar en pos de su propio beneficio.

4. Conclusiones

De acuerdo con lo investigado y desarrollado a lo largo del presente artículo, los autores pueden concluir los siguientes puntos:

a) Los ejercicios de Ataque y Defensa de Equipos Rojo y Azul respectivamente forman parte integral de su desarrollo y mejora, ya que les permite refinar sus estrategias que serán de vital importancia cuando se enfrenten a retos mayores o entre ellos.
b) Los ejercicios de Ataque y Defensa mediante el uso de los diversos equipos son de vital importancia en el campo de la Ciberseguridad debido a que en estos simulacros se pone a prueba los sistemas para comprobar y verificar la solidez de sus defensas e infraestructura, así como la velocidad con la que puede llegar a ser defendida y tratada ante los problemas.
c) El hecho de que existan ejercicios únicos para cada equipo demuestra que la especialización en la forma de trabajar de estos es primordial, ya que permite generar estrategias y métodos para llevar a cabo su tarea de manera satisfactoria ya sea para usarlas en el sistema o entre ellos para ralentizar el progreso del otro equipo.
d) Si bien el foco central reside en los Equipos Rojo y Azul, la labor de todos los demás equipos es igual de importante, y representan otros aspectos del correcto cuidado y protección del sistema, así como sus métodos de respuesta ante el peligro y las direcciones de los defensores, además de ofrecer una correcta gestión del escenario y sistemas involucrados dentro de los ejercicios ya sean estos sistemas reales o prefabricados.

Referencias

Diogenes, Y., & Ozkaya, E. (2018). Cybersecurity: Attack and Defense Strategies. Mumbai: Packt Publishing.

El Universo. (2021). Ciberataque a Banco Pichincha fue realizado por atacantes internacionales, se revela en Comisión de Desarrollo Económico | Economía | Noticias | El Universo. Retrieved from El Universo website: https://www.eluniverso.com/noticias/economia/ciberataque-a-banco-pichincha-fue-realizado-por-atacantes-internacionales-se-revela-en-comision-de-desarrollo-economico-nota/

Fischer, E. A. (2016). Cybersecurity Issues and Challenges. Congressional Research Service, 1–12.

Fuentes-Doria, D. D., Toscano-Hernández, A. E., Malvaceda-Espinoza, E., Díaz Ballesteros, J. L., & Díaz Pertuz, L. (2020). Metodología de la investigación: Conceptos, herramientas y ejercicios prácticos en las ciencias administrativas y contables. Metodología de La Investigación: Conceptos, Herramientas y Ejercicios Prácticos En Las Ciencias Administrativas y Contables. https://doi.org/10.18566/978-958-764-879-9

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and

healthcare: How safe are we? BMJ (Online), 358. https://doi.org/10.1136/bmj.j3179

Ostby, G., Lovell, K. N., & Katt, B. (2019). EXCON teams in cyber security training. Proceedings - 6th Annual Conference on Computational Science and Computational Intelligence, CSCI 2019, 14–19. https://doi.org/10.1109/CSCI49370.2019.00010

Rehberger, J. (2020). Cybersecurity Attacks – Red Team Strategies A Practical Guide to Building a Penetration Testing Program Having Homefield Advantage (P. Publishing, ed.). Mumbai. Retrieved from https://www.google.com.au/books/edition/Cybersecurity_Attacks_Red_Team_Strategie/gtDaDwAAQBAJ?hl=en&gbpv=0

Roussel-Tarbouriech, G. T. H. G. I., Menard, N., True, T., Vi, T., & Reisyukaku. (2019). Methodically Defeating Nintendo Switch Security. Retrieved from http://arxiv.org/abs/1905.07643

Smith, J., Theisen, C., & Barik, T. (2020). A Case Study of Software Security Red Teams at Microsoft. Proceedings of IEEE Symposium on Visual Languages and Human-Centric Computing, VL/HCC, 2020-August. https://doi.org/10.1109/VL/HCC50065.2020.9127203

Straub, J. (2020). Assessment of cybersecurity competition teams as experiential education exercises. ASEE Annual Conference and Exposition, Conference Proceedings, 2020-June. https://doi.org/10.18260/1-2--34187

Yamin, M. M., & Katt, B. (2019). Modeling attack and defense scenarios for cyber security exercises. 5th InterdisciPlinary Cyber Research Conference 2019, 7.

Yamin, M. M., Katt, B., & Nowostawski, M. (2021). Serious games as a tool to model attack and defense scenarios for cyber-security exercises. Computers and Security, 110. https://doi.org/10.1016/j.cose.2021.102450

Zhou, W. C., & Sun, S. L. (2020). Red Teaming Strategy: Huawei's Organizational Learning and Resilience. Palgrave Studies of Internationalization in Emerging Markets, 299–317. https://doi.org/10.1007/978-3-030-47579-6_13