Journal **TechInnovation**
Volumen 2, Número 1, 2023
Universidad Estatal del Sur de Manabí
ISSN-e: 2953-6472

ARTÍCULO DE REVISIÓN

Medios de ataques a los sistemas de seguridad de la información

Means of attacks on information security systems

https://doi.org/10.47230/Journal.TechInnovation.v2.n1.2023.72-78

Recibido: 18-01-2023 **Aceptado:** 21-04-2023 **Publicado:** 01-06-2023

Jonathan Marcelo Conforme Tomala[1]*
https://orcid.org/0000-0002-8813-709X

Evelyn Dayana Bailon Pilozo[2]
https://orcid.org/0000-0003-2019-1222

Luisa Elizabeth Pilozo Pilozo[3]*
https://orcid.org/0000-0001-9306-1352

Mario Javier Marcillo Merino[4]
https://orcid.org/0000-0001-5818-367X

1. Ingeniero en Formación; Facultad de Ciencias Técnicas; Universidad Estatal Del Sur de Manabí; Jipijapa, Ecuador.
2. Ingeniera en Formación; Facultad de Ciencias Técnicas; Universidad Estatal Del Sur de Manabí; Jipijapa, Ecuador.
3. Ingeniera en Formación; Facultad de Ciencias Técnicas; Universidad Estatal Del Sur de Manabí; Jipijapa, Ecuador.
4. Magíster en Docencia Universitaria; Ingeniero en Sistemas; Docente de la Carrera de Tecnologías de la información, Facultad de Ciencias Técnicas; Universidad Estatal Del Sur de Manabí; Jipijapa, Ecuador.

Volumen: 2
Número: 1
Año: 2023
Paginación: 72-78
URL: https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/view/39
***Correspondencia autor:** conforme-jonathan2805@unesum.edu.ec

RESUMEN

La seguridad de los sistemas informáticos es una preocupación fundamental en el mundo digital. Los ataques a los sistemas de seguridad se han convertido en una amenaza constante para las empresas y los usuarios. En esta investigación se describen los diferentes medios de ataque que puedes utilizarse para comprometer la seguridad de un sistema. Entre los medios de ataques se incluyen el phishing, el malware, la ingeniería social, el ataque por fuerza bruta, el ataque de denegación de servicio (DoS), entre otros. Se detallan las características de cada uno de estos medios y se representan medidas preventivas para evitar su éxito. El phishing se refiere a una técnica que consiste en engañar a los usuarios para que revelen información personal o financiera, generalmente a través de correos electrónicos o sitios web falsificados. El malware, por otro lado, es un software malintencionado que se introduce en un sistema para causar daño o robar información. La ingeniería social es una técnica que utiliza la manipulación psicológica para obtener información confidencial. El ataque por fuerza bruta consiste en intentar adivinar contraseñas a través de la repetición de combinaciones de caracteres. El ataque de denegación de servicios (Dos) se enfoca en interrumpir el servicio de un sistema al inundarlo con una gran cantidad de trafico de red. En resumen, es esencial estar al tanto de los diferentes medios de ataques a los sistemas de seguridad y adoptar medidas preventivas para minimizar el riesgo de éxito de estos ataques

Palabras clave: ataques informáticos; ingeniería social; malware; phishing.

ABSTRACT

The security of computer systems is a fundamental concern in the digital world. Attacks on security systems have become a constant threat to companies and users. This research describes the different means of attack that can be used to compromise the security of a system. Attack means include phishing, malware, social engineering, brute force attack, denial of service (DoS) attack, among others. The characteristics of each of these means are detailed and preventive measures are represented to avoid their success. Phishing refers to a technique of tricking users into revealing personal or financial information, usually through spoofed emails or websites. Malware, on the other hand, is malicious software that gets into a system to cause damage or steal information. Social engineering is a technique that uses psychological manipulation to obtain confidential information. The brute force attack consists of trying to guess passwords through the repetition of combinations of characters. The denial of service attack (Dos) focuses on disrupting the service of a system by flooding it with a large amount of network traffic. In summary, it is essential to be aware of the different means of attacks on security systems and take preventive measures to minimize the risk of success of these attacks.

Keywords: computer attacks; social engineering; malware; phishing.

Creative Commons Attribution 4.0 International (CC BY 4.0)

Introducción

El uso de la tecnología es una herramienta fundamental en la vida cotidiana de las personas, empresas y organizaciones en todo el mundo. Sin embargo, el uso de la tecnología también implica riesgos de seguridad informática que pueden poner en peligro la privacidad, la integridad y la disponibilidad de los datos. Los sistemas informáticos son vulnerables a ataques por diferentes medios, y, por lo tanto, es fundamental conocer los distintos tipos de ataques que existen y las medidas preventivas que se pueden tomar para protegerse contra ellos.

El objetivo principal de este articulo científico es identificar los diferentes medios de ataques a los sistemas de seguridad, describir sus características y nuevas amenazas para vulnerar los sistemas de seguridad. Por lo tanto, es fundamental estar al tanto de las nuevas tendencias y evolución de los medios de ataques.

En este artículo se describirán los principales medios de ataques a los sistemas de seguridad, entre ellos el phishing, el malware, la ingeniería social, el ataque por fuerza bruta, el ataque de denegación de servicio (DoS), entre otros. También se presentarán algunas soluciones preventivas y estrategias para minimizar los riesgos de seguridad informática.

Es importante destacar que la seguridad informática es un proceso continuo que implica un esfuerzo constante para proteger los sistemas y los datos. Es necesario establecer medidas preventivas adecuadas y actualizarlas regularmente para asegurarse de que estén protegidos contra las últimas amenazas informáticas. Por lo tanto, es esencial entender los medios de ataques a los sistemas de seguridad para poder adoptar las medidas preventivas necesarias y proteger los sistemas contra ellos.

Los sistemas de seguridad informáticas son herramientas diseñadas para proteger la información y los recursos de las empresas y organizaciones de ataques externos e internos. Sin embargo, con la creciente dependencia de las tecnologías de la información y la comunicación, los ataques informáticos se han convertido en una amenaza cada vez más frecuente y sofisticada (Broadcom Inc. | Connecting Everything, s. f.).

Existen varios medios de ataques que pueden ser utilizado por los atacantes para vulnerar los sistemas de seguridad informática. A continuación, se describen algunos de los más comunes (Alexander S. Gillis et al., 2023).

Ataques de denegación de servicio (DDoS)

Son una amenaza cada vez más común en la seguridad cibernética. Los ataques DDoS tienen como objetivo sobrecargar un sistema o sitio web de destino con un gran número de usuarios legítimos. Esto se logra mediante la utilización de una red de dispositivos comprometidos por los atacantes. Los botnets, que son controlados remotamente por los atacantes. Los botnets pueden incluir dispositivos como computadoras, servidores y dispositivos IoT, lo que los hace extremadamente difíciles de detectar y eliminar.

Mirkovic y Reiher (2005) presentan una taxonomía de ataques DDoS y técnicas de defensa en su artículo "A taxonomy of DDoS attack and DDoS defense mechanisms". Los autores analizan los mecanismos de mitigación disponibles y brindan información detallada sobre la detección y prevención. Los ataques DDoS pueden tener graves consecuencias para las empresas y organizaciones, incluyendo la pérdida de ingresos de datos, la disminución de la reputación y la posible pérdida de datos sensibles. Además, los ataques DDoS a menudo se utilizan como una táctica de distracción para encubrir otros ataques maliciosos que pueden tener lugar simultáneamente.

Para protegerse contra los ataques DDoS, existen diversas técnicas de mitigación disponible, que incluyen el filtrado de paquetes, el equilibrio de carga, la dispersión del DNS y la colaboración entre proveedores de servicios. El filtrado de paquetes implica examinar el tráfico entrante y saliente para bloquear el tráfico malicioso, mientras que el equilibrio de carga distribuye el tráfico en varios servidores para evitar a sobrecarga. La dispersión de DNS implica distribuir la carga de tráfico en múltiples servidores DNS para mitigar los ataques de reflexión y amplificación.

Los ataques DDoS son una amenaza seria en la seguridad cibernética que pueden tener consecuencias graves para las empresas y organizaciones. Es esencial que las empresas tomen medidas de seguridad proactivas y estén actualizadas en las últimas tendencias y técnicas de mitigación para protegerse contra los ataques DDoS y otras formas de ataques cibernéticos.

Ingeniería social

Mitnick y Simon (2003) describen en su libro "The art of deception: Controlling the human element of security" los diferentes tipos de ataques de ingeniería social y cómo los ciberdelincuentes los utilizan para obtener información confidencial de las personas. Los autores proporcionan consejos prácticos sobre cómo protegerse contra estos ataques y mejorar la seguridad en general.

Esta técnica explota la debilidad humana, manipulando a que no son seguras. Los ataques de ingeniería social pueden tomar muchas formas, como la suplantación de identidad, el phishing, la ingeniería inversa y la recolección de información a través de las redes sociales.

La suplantación de identidad implica hacerse pasar por alguien más, como un empleado de una empresa, para obtener información confidencial. El phishing involucra el envío de correos electrónicos o mensajes engañosos que parecen ser legítimos, pero que en realidad son falsos, con el objetivo de obtener información confidencial. La ingeniería inversa implica el análisis de productos o sistemas para obtener información a través de las redes sociales implica el uso de la información disponible públicamente en las redes sociales para obtener información personal.

Para protegerse contra los ataques de ingeniería social, es importante educar a las personas sobre los riesgos y proporcionar capacitación sobre como identificar y evitar estos ataques. También es importante tener políticas de seguridad sólidas y asegurarse de que sigan las prácticas recomendadas para proteger la información confidencial. La combinación de la educación y las políticas de seguridad sólidas puede ayudar a reducir el riesgo de ataques de ingeniería social y proteger la información confidencial.

Malware

Según McDermott (2019), el malware es un software malicioso que puede robar información, dañar el sistema o permitir el acceso no autorizado a los recursos. Los virus, gusanos, troyanos y ransomware son algunos ejemplos de malware comúnmente utilizados por los atacantes. El malware se propaga mediante descargas de software malicioso, correos electrónicos de phishing y otros medios engañosos que engañan a los usuarios para que descarguen e instalen software malicioso. Para protegerse contra el malware, se recomienda utilizar software antivirus y antimalware actualizado y evitar descargar software de fuentes no confiables.

Para protegerse contra el malware, es esencial utilizar software antivirus y antimalware de alta calidad y mantenerlo actualizado. Además, es importante mantener el software del sistema operativo y las aplicaciones actualizado con los últimos parches de

seguridad y evitar descargar software de fuentes no confiables. Los usuarios también deben ser cautelosos al hacer clic en enlaces sospechosos o descargar archivos de correos electrónicos o sitios web desconocidos.

En resumen, el malware es un tipo de software malicioso diseñado para dañar o tomar el control de un sistema informático si el consentimiento del usuario. Los usuarios deben tomar medidas proactivas para protegerse contra el malware, incluyendo el uso de software antivirus y antimalware actualizado, la actualización del software del sistema operativo y las aplicaciones, y la evitación de fuentes no confiables de software y correos electrónicos.

Ataques cibernéticos atreves de fuerza bruta

Deshpande y Patil (2019) explican que el ataque de fuerza bruta es una técnica de hacking utilizada para descifrar contraseñas mediante la generación repetida de intentos hasta que se adivina la contraseña correcta. Para protegerse contra estos ataques, los usuarios deben utilizar contraseñas complejas y únicas que contengan letras mayúsculas, números y caracteres especiales, y se recomienda la autenticación de dos factores. Los administradores de sistemas también deben tomar medidas para proteger sus sistemas, como limitar el número de intentos de inicio de sesión y bloquear direcciones IP después de un número especifico de intentos fallidos.

También se recomienda utilizar la autenticación de dos factores, que requiere una segunda forma de autentificación además de una contraseña, como una huella digital o un código enviado a un teléfono móvil. implementación de medidas de seguridad adicionales, como la autentificación multifactorial, para proteger mejor los sistemas. También es considerado como una técnica de hacking que se utiliza para descifrar contraseñas mediante la generación repetida de intentos. Los usuarios deben utilizar contraseñas complejas y únicas para protegerse contra estos ataques, y los administradores de sistemas deben tomar medidas para proteger sus sistemas, como limitador de intentos de inicio de sesión y la autenticación multifactorial.

Ataques de suplantación de identidad (phishing)

En este estudio, los autores investigan las razones detrás de la efectividad del phishing y cómo los usuarios pueden ser engañados para proporcionar información confidencial a través de correos electrónicos falsos y sitios web fraudulentos. Los resultados muestran que los usuarios a menudo no tienen la capacidad de distinguir entre sitios web legítimos y fraudulentos, y sugieren formas en que los diseñadores de sitios web pueden mejorar la seguridad y la privacidad de los usuarios (Dhamija, R., Tygar, J. D., & Hearst, M. 2006).

Materiales y Métodos

Los materiales que se abordaron en este trabajo de investigación fueron: fuentes bibliográficas lo que conlleva a una investigación completa y sólida. En cuanto a los métodos que se usaron se destacan el análisis-síntesis, histórico-lógico, bibliográfico-documental, los cuales permitieron sintetizar las indagaciones, facilitando una búsqueda más precisa sobre el tema medios de ataques.

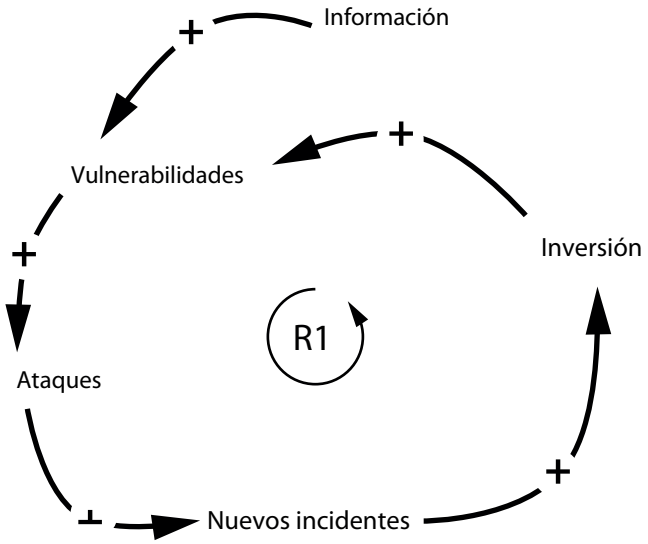
Resultados y Discusión

Mediante el análisis de los medios de ataques a los sistemas de seguridad de la información, tomando en consideración las investigaciones de las técnicas OSINT la que mayor efectividad puede tener en el proceso es OCTAVE este cuenta con procesos de evaluación y análisis de acuerdo

a las amenazas y vulnerabilidades. Amenazas que afectan a los sistemas de información Alertas de amenazas La seguridad informática, de igual manera a como sucede con la seguridad aplicada a otros entornos, trata de minimizar los riesgos asociados al acceso y utilización de determinados sistemas de forma no autorizada y en general malintencionada. El objetivo de la seguridad informática es proteger los recursos informáticos valiosos de la organización, tales como información, hardware o software. A través de la adopción de las medidas adecuadas, la seguridad informática ayuda a una organización a cumplir sus objetivos, permite proteger los recursos financieros, sistemas de información, reputación, situación legal, y otros bienes tanto tangibles e intangibles.

En efecto, gestionar la seguridad informática organizacional es una tarea exigente y evaluar el valor de las tecnologías de seguridad es esencial para gestionar eficazmente la seguridad de la información. El modelo presenta el diagrama causal de una empresa sin medidas de seguridad, la cual actúa únicamente en caso de que un ataque se convierta en un incidente. Las variables consideradas en este escenario son: tasa información, vulnerabilidades, ataques, nuevos incidentes, e inversión como se muestra en la siguiente imagen:

Figura 1. Empresa sin seguridad informática



Fuente: (Amaya Balaguera, 2015).

Nota: Ejemplo de proceso de una empresa de seguridad informática. Según (Amaya Balaguera, 2015). Si se invierte en solventar el ataque, no se resuelve el problema porque se descuida otro donde sí se debería invertir, ya que no se tiene un plan definido y no se conocen las necesidades de seguridad, lo que aumenta la vulnerabilidad porque se invierte en algo que no requería mayor atención y se deja de hacer en otra que sí.

Conclusiones

Los ataques pueden ser de diferentes tipos:

Los ataques pueden ser realizados mediante técnicas como el phishing, la ingeniería social, el malware, el ransomware, el spyware, entre otros. Cada tipo de ataque tiene como objetivo vulnerar un aspecto específico del sistema de seguridad, por lo que es importante contar con medidas de protección adecuadas para prevenirlos.

La seguridad de los sistemas debe ser integral:

La seguridad de los sistemas no solo depende de las medidas de protección que se implementen, sino mantenimiento del sistema y se educan a los usuarios en cuanto a buenas prácticas de seguridad. Es importante considerar todos estos aspectos para garantizar la seguridad de los sistemas.

Bibliografía

Shea, S., Gillis, A. S., & Clark, C. (2023, 11 enero). What is cybersecurity? Security. https://www.techtarget.com/searchsecurity/definition/cybersecurity

Mirkovic, J., & Reiher, P. (2005). A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 35(2), 39-53.

Mitnick, K., & Simon, W. L. (2003). The art of deception: Controlling the human element of security. John Wiley & Sons.

McDermott, J. P. (2019). Malware. En The cybersecurity handbook: A guide for achieving optimal enterprise cybersecurity readiness (pp. 111-124). Wiley.

Deshpande, M., & Patil, A. (2019). Brute Force Attack and its Mitigation Techniques: A Review. International Journal of Computer Applications, 179(25), 39-44.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 581-590). ACM.

Amaya Balaguera, Y. D. (2015). Metodologías ágiles en el desarrollo de aplicaciones para dispositivos móviles. Estado actual. Revista de Tecnología, 12(2). https://doi.org/10.18270/rt.v12i2.1291

Cómo citar: Conforme Tomala, J. M., Bailon Pilozo, E. D., Pilozo Pilozo, L. E., & Marcillo Merino, M. J. (2023). Medios de ataques a los sistemas de seguridad de la información . Journal TechInnovation, 2(1), 72–78. https://doi.org/10.47230/Journal.TechInnovation.v2.n1.2023.72-78