Adopción de pautas de seguridad informática (Seguridad y alta disponibilidad)

Fiabilidad, confidencialidad, integridad y disponibilidad

- **Fiabilidad**: probabilidad de que un sistema se comporte tal y como se espera de él.
- **Confidencialidad**: acceso a la información solo mediante autorización y control.
- **Integridad**: la información solo mediante autorización.
- **Disponibilidad**: la información del sistema es accesible mediante autorización.

Más información

- https://www.jesusninoc.com/01/10/curso-de-hacking-con-powershell/
- https://www.jesusninoc.com/02/28/seguridad-informatica-con-powershell/#Introduccion

---

Elementos vulnerables en el sistema informático: hardware, software y

datos

- **Hardware**: elementos físicos del sistema informático, tales como procesadores, electrónica y cableado de red, medios de almacenamiento (cabinas, discos, cintas, DVDs,…).
- **Software**: elementos lógicos o programas que se ejecutan sobre el hardware, tanto si es el propio sistema operativo como las aplicaciones.
- **Datos**: comprenden la información lógica que procesa el software haciendo uso del hardware. En general serán informaciones estructuradas en bases de datos o paquetes de información que viajan por la red.

Análisis de las principales vulnerabilidades de un sistema informático

Definimos vulnerabilidad como debilidad de cualquier tipo que compromete la seguridad del sistema informático.

Top 10 Web Application Security Risks

- Injection. Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
- Broken Authentication. Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users’ identities temporarily or permanently.
- Sensitive Data Exposure. Many web applications and APIs

do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

- XML External Entities (XXE). Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
- Broken Access Control. Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
- Security Misconfiguration. Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.
- Cross-Site Scripting (XSS). XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
- Insecure Deserialization. Insecure deserialization often

leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

- Using Components with Known Vulnerabilities. Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
- Insufficient Logging & Monitoring. Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Amenazas. Tipos

Amenazas físicas

Dentro de las amenazas físicas podemos englobar cualquier error o daño en el hardware que se puede presentar en cualquier momento. Por ejemplo, daños en discos duros, en los procesadores, errores de funcionamiento de la memoria, etc. Todos ellos hacen que la información o no esté accesible o no sea fiable.

Amenazas lógicas

El punto más débil de un sistema informático son las personas relacionadas en mayor o menor medida con él. Puede ser inexperiencia o falta de preparación, o sin llegar a ataques

intencionados propiamente, simplemente sucesos accidentales. Pero que, en cualquier caso, hay que prevenir.

Más información

- https://www.jesusninoc.com/10/16/enviar-paquetes-de-desasociacion-con-aireplay-ng-a-un-cliente-que-actualmente-esta-asociado-con-un-punto-de-acceso-en-linux-realizando-una-conexion-ssh-desde-powershell-en-windows/
- https://www.jesusninoc.com/02/17/ataques-dos/
- https://www.jesusninoc.com/02/01/crear-un-dominio-onion/
- https://www.redteamsecure.com/evil-svg-project/
- https://www.hacklooking.cl/2019/01/13/kali-linux-tor-desde-tu-navegador-y-sin-instalar-nada/
- https://www.jesusninoc.com/02/01/crear-un-dominio-onion/
- https://www.jesusninoc.com/11/10/realizar-conexiones-tcp-udp-con-powershell/

Seguridad física y ambiental

Ubicación y protección física de los equipos y servidores

Hay que tener en cuenta que cuando existe acceso físico a un recurso ya no existe seguridad sobre él. Supone entonces un gran riesgo y probablemente con un impacto muy alto.

Sistemas de alimentación ininterrumpida

Puede ocurrir un incendio o un apagón y no tener bien definidas las medidas a tomar en estas situaciones o simplemente no tener operativo el SAI que debería responder de forma inmediata al corte de suministro eléctrico.

Sistemas de alimentación ininterrumpida, en inglés uninterruptible power supply, es un dispositivo que gracias a sus baterías y otros elementos almacenadores de energía, durante un apagón eléctrico puede proporcionar energía eléctrica por un tiempo limitado a todos los dispositivos que tenga conectados.

Seguridad lógica

Criptografía

La criptografía se ha definido, tradicionalmente, como el ámbito de la criptología que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

Más información

- https://www.jesusninoc.com/02/17/ejercicios-de-seguridad-detectar-mediante-firmas-que-un-fichero-se-ha-infectado/
- https://www.jesusninoc.com/02/17/ejercicios-de-seguridad-adivinar-un-hash-utilizando-un-fichero-con-hashes-generados/
- https://www.jesusninoc.com/02/28/seguridad-informatica-con-powershell/#Criptografia
- https://www.jesusninoc.com/2017/11/06/creates-a-new-self-signed-certificate/
- https://www.jesusninoc.com/2017/11/10/encrypts-content-by-using-the-cryptographic-message-syntax-format/
- https://www.jesusninoc.com/2017/11/12/decrypts-content-that-has-been-encrypted-by-using-the-cryptographic-message-syntax-format/
- https://www.jesusninoc.com/2017/11/18/exports-a-certific

ate-to-a-personal-information-exchange-pfx-file/

- https://www.jesusninoc.com/2017/11/20/imports-certificates-and-private-keys-from-a-personal-information-exchange-pfx-file-to-the-destination-store/
- https://www.jesusninoc.com/01/23/cifrar-con-un-algoritmo-sencillo-el-nombre-y-el-contenido-de-un-fichero-de-texto/

Listas de control de acceso

En seguridad informática, una lista de control de acceso es una lista de permisos asociados con un recurso del sistema. Una ACL especifica qué usuarios o procesos del sistema tienen acceso a los objetos, así como qué operaciones están permitidas en determinados objetos.

Establecimiento de políticas de contraseñas

Una política de contraseñas es un conjunto de reglas diseñadas para mejorar la seguridad informática al alentar a los usuarios a emplear contraseñas seguras y usarlas correctamente.

Más información

- https://www.jesusninoc.com/contrasenas-seguras-con-powershell/

Políticas de almacenamiento

Las políticas de almacenamiento son normas de almacenamiento para los equipos de trabajo (equipos de sobremesa, equipos portátiles, teléfonos y otros dispositivos) que los usuarios deben cumplir.

Esta política incluye al menos los siguientes aspectos:

- Qué tipo de información se puede almacenar en los equipos locales.
- Cuánto tiempo debe permanecer dicha información en los mismos.
- Permanencia de la información en la red local una vez transmitida a los servidores corporativos.
- Ubicación dentro del árbol de directorios del equipo.
- Utilización de sistemas de cifrado de información en los documentos empresariales.
- Normativa para los empleados relativa al almacenamiento de documentos personales, archivos de música, fotografías, etc., y en concreto relativa a archivos que estén bajo algún tipo de regulación en cuanto a derechos de autor (descargas desde los equipos de trabajo).

Más información

- https://www.jesusninoc.com/11/16/10-gestion-del-rendimiento-en-powershell-para-administradores-de-sistemas/#Copias_de_seguridad
- https://www.jesusninoc.com/02/12/algoritmo-de-descifrado-sencillo/
- https://www.jesusninoc.com/02/12/comprimir-archivo/

Copias de seguridad e imágenes de respaldo

Una copia de seguridad consiste simplemente en tener duplicados los archivos en algún dispositivo o medio de almacenamiento, los archivos pueden ser de los usuarios o propios del sistema operativo con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados.

Tipos de copias de seguridad:

- **Copia completa.** Se almacenan todos los archivos de los que se desea hacer copia y se marcan como copiados. Este tipo de copia requiere gran cantidad de tiempo y suficiente espacio de almacenamiento para guardar la copia.
- **Copia incremental (progresiva).** Se almacenan los archivos que se han modificado desde la última copia completa o incremental y se marcan como copiados.
- **Copia diferencial.** Se almacenan los archivo que se han modificado desde la última copia completa y no se marcan como copiados.

Todo plan de contingencia de una empresa requiere contar con una planificación adecuada de las copias de seguridad que se realizan, ya que la pérdida de datos puede poner en peligro la continuidad del negocio.

Una imagen de respaldo consiste en hacer una copia de la totalidad de información que contiene el sistema operativo, es decir, de los programas, de las aplicaciones y de tu sistema operativo.

Más información

- https://www.jesusninoc.com/11/16/10-gestion-del-rendimiento-en-powershell-para-administradores-de-sistemas/#Copias_de_seguridad

---

Medios de almacenamiento

El soporte de almacenamiento de datos o medio de almacenamiento de datos es el material físico donde se almacenan los datos que pueden ser procesados por una computadora, un dispositivo electrónico, y un sistema informático, aunque este término también abarca el concepto de documento no necesariamente informatizable.

Más información

- http://www.developandsys.es/aseguramiento-la-informacion/

Análisis forense en sistemas informáticos

El análisis forense en un sistema informático es una ciencia moderna que permite reconstruir lo que ha sucedido en un sistema tras un incidente informático.

Más información

- https://www.jesusninoc.com/02/28/seguridad-informatica-con-powershell/#Forense

- https://www.jesusninoc.com/09/12/crear-un-fichero-de-volcado-de-memoria-de-un-proceso-y-buscar-una-cadena/
- https://www.jesusninoc.com/11/28/crear-compilar-y-ejecutar-una-dll-con-microsoft-visual-c-que-abre-notepad-desde-powershell/
- https://www.jesusninoc.com/02/05/crear-un-usuario-local-con-contrasena-en-windows-10/
- https://www.jesusninoc.com/11/29/crear-compilar-y-ejecutar-una-dll-con-microsoft-visual-c-que-crear-un-usuario-desde-powershell/
- https://www.jesusninoc.com/01/27/comprobar-si-ha-cambiado-algun-fichero-utilizando-la-funcion-hash-sha1/
- https://www.jesusninoc.com/10/22/crear-un-fichero-de-volcado-de-memoria-de-un-proceso-y-detectar-dll/
- https://www.jesusninoc.com/10/21/analizar-un-fichero-exe-con-floss/
- https://www.jesusninoc.com/11/26/crear-compilar-y-ejecutar-una-dll-con-microsoft-visual-c-que-ejecute-un-cmdlet-de-powershell/
- https://www.jesusninoc.com/04/19/listar-funciones-exportadas-de-un-archivo-dll-con-dumpbin-desde-powershell/
- https://www.jesusninoc.com/04/21/obtener-los-nombres-de-las-funciones-exportadas-de-un-archivo-dll-con-dumpbin-desde-powershell-explicacion-paso-a-paso-del-script/
- https://www.jesusninoc.com/07/07/vaciar-y-restablecer-el-contenido-de-la-cache-de-resolucion-del-cliente-dns-en-windows-10/
- https://www.jesusninoc.com/03/04/crear-un-fichero-de-volcado-de-memoria-de-un-proceso/
