Exposición INFORMÁTICA

Camila Alonso, Ludmila Galván,

morena Zenteno y Liz Anes

12/11/24

Escaneo de puertos

Un escaneo de puertos es una técnica común que los piratas informáticos utilizan para descubrir puertas abiertas o puntos débiles en una red. Un ataque de escaneo de puertos ayuda a los ciberdelincuentes a encontrar puertos abiertos y averiguar si están recibiendo o enviando datos.

https://www.fortinet.com/lat/resources/cyberglossary/what-is-port-scan

BackDoors

En informática un backdoor es un tipo de virus diseñado para dar acceso a usuarios maliciosos al control de un equipo infectado de manera remota. Estas "puertas traseras" permiten al usuario malicioso controla el equipo infectado, pudiendo enviar y recibir archivos, ejecutarlos o eliminarlos, mostrar mensajes, borrar o robar datos, reiniciar el equipo, etc. Es decir, puede controlar el equipo como si estuviese sentado delante de él y a los mandos.

https://protecciondatos-lopd.com/empresas/backdoor/

Troyano

- Un virus troyano es un tipo de malware que se descarga en una computadora disfrazado de programa legítimo. El método de entrega suele hacer que un atacante utilice la ingeniería social para ocultar código malicioso dentro del software legítimo para intentar obtener acceso al sistema de los usuarios con su software.

https://youtu.be/UlmxHFQtMhI?si=K5sErM6pXSAIzoKC

Sniffing

El sniffing es un tipo de ciberataque que tiene lugar cuando los paquetes que pasan por una red son monitorizados, capturados y, a veces, analizados

https://youtu.be/sxg4sCjdz84?si=hRkI4wjE9sWRf-nD

Ransomware

El ransomware es un tipo de software malicioso, o malware, que bloquea archivos y datos y los retiene para pedir un rescate. Suele hacerlo mediante la encriptación de los archivos y datos, y el atacante se queda con la clave de encriptación.

https://youtu.be/SC8cqQfq9zk?si=m94DSiAJVK0Vw_IV

Código malicioso

¿Qué es el código malicioso o malware? Son programas que tienen como objetivo acceder a tu sistema sin que detectes su presencia. En función de la intención del Cracker, el programa podría: Robar credenciales, datos bancarios, información

https://youtu.be/E3DW7OUf2SM?si=PiHUfnpFMb-hLtRQ

Hacker

- alguien que utiliza sus habilidades para descubrir nuevas formas de usar los sistemas y resolver problemas

Spoofing

El spoofing, o suplantación de identidad, es un conjunto de técnicas que utilizan los atacantes para hacerse pasar por una persona o entidad de confianza y engañar a las víctimas.

Denegación de servicio

Un ataque de denegación de servicio (DoS) es un ciberataque que se produce cuando un actor malicioso envía una gran cantidad de solicitudes o tráfico a un servidor o red, con el objetivo de que un dispositivo o ordenador no esté disponible para los usuarios.

Ataques de contraseña

Los ataques a contraseñas son una forma de ataque cibernético que se realiza con el objetivo de obtener acceso no autorizado a sistemas. Los actores de amenazas pueden realizar estos ataques por diversas razones, como hurtos menores o actos de guerra.

Eavesdropping

El eavesdropping de red es un ataque de capa de red que se enfoca en capturar pequeños paquetes de la red transmitidos por otros computadores y leer el contenido de datos en la búsqueda de cualquier tipo de información.

Exploit

programa, secuencia de comandos o fragmento de datos que se aprovecha de una vulnerabilidad o error para provocar un comportamiento no deseado en un sistema, hardware o software.

White hat

El término White Hat Hacker o hacker de sombrero blanco en Internet se refiere a un hacker ético, o un experto de seguridad informática, quien se especializa en pruebas de penetración y en otras metodologías para detectar vulnerabilidades

Ciberataque

Un ciberataque es un conjunto de acciones dirigidas contra sistemas de información, como pueden ser bases de datos o redes computacionales, con el objetivo de perjudicar a personas, instituciones o empresas.

Trashing

El trashing es la acción de obtener información a través de archivos y documentos desechados o descartados; con la finalidad de cometer fraudes y robos de identidad.

Adware

Un adware es un tipo de programa publicitario malicioso. Su nombre proviene de la combinación de las palabras en inglés ad (advertising o publicidad) y ware (que alude a software o programa informático).

Software

Cuando hablamos de software ilegal o "pirata" como se conoce comúnmente, nos referimos a un programa que ha sido duplicado, distribuido e instalado sin autorización del fabricante quien cuenta con los derechos de autor registrados.

Control remoto de equipos (de forma maliciosa)

Un troyano de acceso remoto (o RAT, del inglés Remote Access Trojan) es una herramienta que los desarrolladores de malware usan para obtener acceso total y controlar remotamente al sistema de un usuario, incluyendo su teclado y su ratón, acceso a sus archivos y a sus recursos de red.

Criptografía

Qué es la criptografía y para qué sirve?

La criptografía es una práctica que consiste en proteger información mediante el uso de algoritmos codificados, hashes y firmas

Daños físicos

Los daños físicos pueden describirse como los daños resultantes de que el recubrimiento magnético de los platos del disco duro se dañe o se destruya.

Defacement

El defacement es un tipo de ataque que se realiza contra un sitio web, en el que se modifica la apariencia de alguna de sus páginas, para llevar a cabo algún tipo de acción fraudulenta o de vandalismo.

Spyware

El spyware es un tipo de software que se instala en el ordenador sin que el usuario tenga constancia de ello. Suele venir oculto junto a otros programas que se instalan de manera consciente, lo que lo hace muy difícil de detectar. Una vez en el ordenador, recopila información para enviarla a terceros.

Phishing

¿Qué es y cómo funciona el phishing?

El phishing es una técnica de ingeniería social que consiste en el envío de correos electrónicos que suplantan la identidad de compañías u organismos públicos y solicitan información personal y bancaria al usuario.

Muchas GRACIAS por su atención...