TRABAJO PRÁCTICO DE VIRUS

Nombre y apellido: Bustos Bianca y Evelin Orquera

3°A

Colegio del Prado

Phishing: es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o

Escaneo de puertos: servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.

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.

Criptografia: 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 incomprensibles a receptores no autorizados.

Backdoor: Una puerta trasera o Backdoor es un método utilizado para sortear las barreras de autentificación y encriptación de un ordenador y crear un acceso secreto que permita acceder y controlar un equipo o dispositivo sin que el usuario se dé cuenta.

Ramsodware: Estas son algunas señales que permiten detectar un ataque de ransomware: Alertas del antivirus. La aplicación antivirus del dispositivo (si nada ni nadie la ha deshabilitado) puede ser la primera en detectar una infección de ransomware. Cambios en las extensiones de los archivos.

Troyano informática, se denomina caballo de Troya, o troyano, a un malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.

Sniffing: También denominado rastreador de red, es un software o hardware que se utiliza para monitorizar, capturar y analizar en tiempo real los paquetes de datos que

pasan por una red, sin redirigirlos ni alterarlos. Aunque originalmente no es una herramienta maliciosa, es posible utilizarla como tal.

Código malicioso : 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...

Daño físico al equipamiento: En qué consisten los daños físicos en los dispositivos? 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. Estos daños pueden producirse en cualquier dispositivo de almacenamiento con piezas móviles.

Spoofing: Un ejemplo de spoofing de correo electrónico sería un caso en que un atacante crea un correo electrónico que parezca que proviene de PayPal. El mensaje le dice al usuario que su cuenta se suspenderá si no hace clic en un enlace, autentica su identidad en la página y cambia la contraseña de la cuenta.

Hackers:Un hacker, en el sentido tradicional y ético, es alguien que utiliza sus habilidades para descubrir nuevas formas de usar los sistemas y resolver problemas. Un cracker, por otro lado, es un individuo que rompe los sistemas de seguridad, generalmente con intenciones maliciosas.

Exploit: un programa informático, una parte de un software o una secuencia de comandos que se aprovecha de un error o vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, hardware o en cualquier dispositivo electrónico.

Eavesdropping: 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. Este tipo de ataque de red es normalmente muy efectivo cuando no hay uso de encriptación.

Ataque de contraseña:Un ataque de pulverización de contraseñas es un tipo de ataque de fuerza bruta. Se dirige a varias cuentas de usuario con unas pocas contraseñas de uso común, en lugar de intentar muchas contraseñas contra una sola cuenta de usuario.

Denegación de servicio:Un ataque de denegación de servicio (DoS) es un tipo de ciberataque en el que un actor malicioso tiene como objetivo que un ordenador u otro dispositivo no esté disponible para los usuarios a los que va dirigido, interrumpiendo el funcionamiento normal del mismo.

Fraude informatico: Es un delito que comete el que manipula un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o lo hace a través de cualquier interferencia en el funcionamiento de un sistema informático

Malware: El software malicioso, o malware, es cualquier código de software o programa informático, incluidos ransomware, troyanos y spyware, escrito intencionadamente para dañar los sistemas informáticos o a sus usuarios. Casi todos los ciberataques modernos implican algún tipo de malware.

Software ilegal: ¿Qué es el uso ilegal del software?

El concepto de software ilegal o pirata se refiere a la falsificación o copia no autorizada de un programa informático con derechos de autor registrados, que no cuenta con la correspondiente licencia para su uso de manera legal.

Adware: es un tipo de programa p Ataques ublicitario 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).

Control remoto de equipos: El acceso remoto es la capacidad de acceder a un ordenador o dispositivo desde otro dispositivo, en cualquier momento y desde cualquier lugar.

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.

Ciberataque: es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital.

White hat:SEO se refiere a las prácticas éticas y conformes a las pautas de los motores de búsqueda, mientras

Spyware: es un software que se instala sin tu consentimiento informado, ya sea un ordenador tradicional, una aplicación en el navegador web o una aplicación móvil que se encuentra en tu dispositivo. En resumen, el spyware se comunica información personal confidencial sobre ti a un atacante.

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.