Virus informaticos

25 tipos de virus

1	Phishing
2	Escaneo de Puertos
3	Criptografía
4	Backdoors
5	Ransomware
6	Troyano
7	Sniffing
8	Código Malicioso
9	Daños Físicos al Equipamiento
10	Spoofing
11	Hackers
12	Exploit
13	Eavesdropping
14	Ataques de Contraseña
15	Denegación de Servicio
16	Fraude Informático
17	Malware
18	Software ilegal
19	Adware
20	Control Remoto de Equipos (forma maliciosa)
21	Trashing
22	Ciberataque
23	White hat
24	Spyware
25	Defacement

Phishing

El phishing es una técnica de ciberdelincuencia que consiste en enviar correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos para robar información confidencial. El objetivo es que los usuarios compartan datos como contraseñas, números de tarjetas de crédito, información de cuentas bancarias, entre otros, para utilizarlos o venderlos.

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 es una disciplina de la ciberseguridad que se encarga de proteger la información y las comunicaciones mediante el uso de algoritmos codificados, hashes y firmas. Su objetivo es que solo las personas autorizadas puedan acceder a los datos.

Backdoors

Una puerta trasera es una secuencia especial dentro del codigo de promagacion mediante la cual se pueden evitar los sistemas de seguridad del algorithm para acceder al sistema

Ransware

Es un tipo de programa dañino que restringe el acceso determinadas partes o archivos del sistema

Troyano

Es un tipo de malware que sea presenta Como un programa legitimo pero es un software malicioso que permite acceder al sistema del usuario

Sniffing

Sniffing es el proceso de capturar y examinar el tráfico de red, incluyendo datos, correos electrónicos, contraseñas y otra información confidencial, sin ser detectado..

Codigo

Código malicioso (malware) se refiere a cualquier tipo de software o código diseñado para dañar, interferir o explotar sistemas informáticos, redes o ddispositivo

Malware

El malware (abreviatura de "malicious software" o "software malicioso") se refiere a cualquier tipo de software diseñado para dañar o realizar acciones no deseadas en un sistema informático, redes o dispositivos.

Spyware: Software malicioso que espía y recopila información confidencial sin consentimiento.

Trashing:Ataque cibernético que sobrecarga un sistema o red con tráfico no deseado, afectando su funcionamiento.

Adware:* Software malicioso que muestra anuncios no deseados.

La denegación de servicio (DoS, por sus siglas en inglés) :es un tipo de ataque cibernético que busca hacer que un sistema, red o recurso informático sea inaccesible o dejar de funcionar correctamente, sobrecargándolo con una cantidad masiva de tráfico o solicitudes.

[Eavesdropping (:escucha clandestina) es la interceptación y escucha no autorizada de conversaciones privadas, comunicaciones electrónicas o datos transmitidos. Puede ser realizada por individuos, organizaciones o gobiernos.

.: El fraude informático :se refiere a cualquier tipo de estafa o engaño que se realiza utilizando tecnologías informáticas y redes de comunicación.

¡Muchas gracias!