ABC DEL HACKING

A

ADWARE

ES UN SOFTWARE NO DESEADO DISEÑADO PARA MOSTRAR ANUNCIOS EN LA PANTALLA, DE UN DISPOSITIVO.

B

BOTNET

ES UNA RED DE "BOTS" QUE EL DELINCUENTE PUEDE ADMINISTRAR DE FORMA REMOTA.

C

CIFRADO

ES UN PROCESO DE CODIFICACIÓN DE UN MENSAJE O INFORMACIÓN PARA QUE SEA ILEGIBLE Y SECRETO.

D

DDOS

SE TRATA DE UNA TÉCNICA DE DENEGACIÓN DE SERVICIO QUE UTILIZA NUMEROSOS HOSTS PARA REALIZAR EL ATAQUE.

E

EXPOSICIÓN

ES LA COMBINACIÓN DE LOS NIVELES DE PROBABILIDAD E IMPACTO DE UN RIESGO.

F

FUERZA BRUTA

ES UN MÉTODO DE PRUEBA Y ERROR PARA DESCIFRAR DATOS COMO CONTRASEÑAS U OTRA INFORMACIÓN CIFRADA.

G

GUSANO

ES UN PROGRAMA AUTÓNOMO DESTRUCTIVO QUE PUEDE AUTORREPLICARSE.

H

HACKER

ES USUARIO NO AUTORIZADO QUE INTENTA U OBTIENE ACCESO A UN SISTEMA DE INFORMACIÓN.

I

INFILTRADO

ES UNA PERSONA CON INFORMACIÓN PRIVILEGIADA QUE UTILIZA SU ACCESO PARA DAÑAR LA SEGURIDAD DE UNA ORGANIZACIÓN.

J

JAMMING

SE TRATA DE UN ATAQUE QUE INTENTA INTERFERIR CON LA RECEPCIÓN DE COMUNICACIONES DE DIFUSIÓN.

K

KEY LOGGER

ES UN PROGRAMA DISEÑADO PARA OBTENER CONTRASEÑAS O CLAVES DE CIFRADO Y ASÍ ELUDIR OTRAS MEDIDAS DE SEGURIDAD.

L

LISTA NEGRA

SE TRATA DE UNA LISTA DE ENTIDADES, COMO HOSTS O APLICACIONES QUE ESTÁN ASOCIADAS CON ACTIVIDAD MALICIOSA.

M

MAN IN THE MIDDLE

ES UN ATAQUE EN EL QUE SE ADQUIERE LA CAPACIDAD DE LEER, INSERTAR Y MODIFICAR A VOLUNTAD.

N

NETWORK SNIFFING

ES UNA TÉCNICA PASIVA QUE SUPERVISA LA COMUNICACIÓN DE LA RED, DECODIFICA Y EXAMINA EN BUSCA DE INFORMACIÓN.

O

OBSCURED DATA

SON DATOS QUE HAN SIDO DISTORSIONADOS POR MEDIOS CRIPTOGRÁFICOS U OTROS PARA OCULTAR INFORMACIÓN.

P

PHISHING

ES UNA TÉCNICA DE INGENIERÍA SOCIAL QUE SE UTILIZA PARA ROBAR INFORMACIÓN A TRAVÉS DEL CORREO ELECTRÓNICO.

Q

QUADRANT

ES LA TECNOLOGÍA QUE BRINDA PROTECCIÓN A PRUEBA DE MANIPULACIONES A LOS EQUIPOS CRIPTOGRÁFICOS.

R

ROOTKIT

ES UN MÉTODO UTILIZADO PARA REALIZAR UNA INTRUSIÓN CIBERNÉTICA, QUE ES DIFÍCIL DE DETECTAR.

S

SUPLANTACIÓN DE IDENTIDAD

ES CUANDO ALGUIEN OBTIENE Y UTILIZA INDEBIDAMENTE LOS DATOS PERSONALES DE OTRA PERSONA.

T

THREAT SHIFTING

ES LA RESPUESTA DE LOS ADVERSARIOS A LAS CONTRAMEDIDAS DE LOS DEFENSORES PARA EVITAR SER DETECTADOS.

U

UDDI

ES UN SERVICIO DE BÚSQUEDA BASADO EN XML PARA UBICAR SERVICIOS WEB EN UNA TOPOLOGÍA DE INTERNET.

V

VIOLACIÓN DE DATOS

ES LA EXPOSICIÓN DE INFORMACIÓN Y ARCHIVOS CONFIDENCIALES A PERSONAS NO AUTORIZADAS.

W

WEB BUG

ES CÓDIGO MALICIOSO COLOCADO EN SITIOS WEB QUE PERMITE RASTREAR EL USO DE SERVIDORES WEB Y RECOPILAR INFORMACIÓN.

X

XML

SE TRATA DE UN FORMATO DE TEXTO FLEXIBLE DISEÑADO PARA DESCRIBIR DATOS PARA PUBLICACIÓN ELECTRÓNICA..

Y

YAML

ES UN FORMATO DE SERIALIZACIÓN DE DATOS LEGIBLE POR HUMANOS INSPIRADO EN LENGUAJES COMO XML, C, PYTHON, PERL.

Z

ZERO DAY ATTACK

SE TRATA DE UN ATAQUE QUE EXPLOTA UNA VULNERABILIDAD DE HARDWARE, FIRMWARE O SOFTWARE PREVIAMENTE DESCONOCIDA.

FUENTES: - NIST 2022 "COMPUTER SECURITY RESOURCES CENTER
- ASTRA 2022 "20 MUST-KNOW HACKING TERMINOLOGIES TO SAFEGUARD YOUR ONLINE BUSINESS FROM HACKERS"

Grupo Smartekh

PARA MÁS INFORMACIÓN ENTRA A:

WWW.SMARTEKH.COM