Conciencia sobre Ciberseguridad modulo 3 Cheat Sheet

by gonax133 via cheatography.com/211069/cs/45717/

Malware

El malware es un software intrusivo diseñado por ciberdelincuentes para robar datos o dañar sistemas (Cisco).

Tipos de malware

Adware	Muestra anuncios no deseados en tu pantalla.
Spyware	Observa tu actividad en el computador y la reporta al atacante.
Viruses	Infecta archivos o áreas del sistema y se propaga replicándose a sí mismo.
Gusanos	Se propaga replicándose a sí mismo sin la acción del usuario.
Troyanos	Se hace pasar por software legítimo mientras ejecuta acciones maliciosas.
Ransomware	Cifra sistemas y datos, exigiendo un rescate para la descifrado.
Rootkit	Obtiene acceso de administrador y es difícil de eliminar.
Keyloggers	Programas que registran las pulsaciones de teclas.
Minadores de criptomonedas maliciosos	Usan tu computadora para minar criptomonedas para los atacantes.

Cómo obtener malware

1) Abrir un archivo adjunto malicioso en un correo electrónico.
2) Visitar sitios web inseguros.
3) Descargar archivos de fuentes no confiables.
4) Hacer clic en enlaces maliciosos en mensajes (por ejemplo, WhatsApp, Facebook).
5) Usar USBs, tarjetas SD o CDs desconocidos.

Nunca uses memorias USB que hayas encontrado en áreas comunes. Podrían haber sido plantadas allí intencionalmente con la esperanza de que las inserts en tu computadora.

Ataques de día cero

Un ataque de día cero explota una vulnerabilidad desconocida en hardware, firmware o software, sin una solución inmediata disponible.

Amenaza persistente avanzada

Una Amenaza Persistente Avanzada (APT) es un ataque a largo plazo y sigiloso en redes llevado a cabo por estados-nación, grupos patrocinados por el estado o crimen organizado, con el objetivo de obtener inteligencia, beneficios militares o financieros.

Viruses

Según CISA, un virus infecta archivos o áreas del sistema y se replica a sí mismo.

Síntomas de un virus

Rendimiento lento	Archivos corruptos o faltantes	Ventanas emergentes y adware
Fallos de programas y del sistema operativo	Disco duro giratorio	Malfuncionamientos del sistema

Efectos:
Información personal robada y Pérdida de acceso a cuentas

Ransomware

Malware que cifra archivos, haciendo que estos y los sistemas relacionados sean inutilizables.
El ransomware cifra archivos, exigiendo un pago para su descifrado. Es una amenaza importante para todas las industrias, y a menudo se propaga a través de correos electrónicos de phishing con archivos adjuntos maliciosos.

Ataques de Denegación de Servicio (DoS)

Un ataque de Denegación de Servicio (DoS) interrumpe sistemas, dispositivos o redes al abrumarlos con tráfico, impidiendo el acceso legítimo. Esto puede detener las operaciones comerciales, afectar servicios como correos electrónicos, sitios web y mensajería, y resultar en pérdidas financieras. Los atacantes pueden estar motivados por ganancias financieras, hacktivismo o intentos de acceso a sistemas.

Denegación de Servicio Distribuida (DDoS)

Un ataque de Denegación de Servicio Distribuida (DDoS) ocurre cuando múltiples dispositivos secuestrados abrumen un sistema objetivo. Los atacantes explotan vulnerabilidades para controlar estos dispositivos y dirigirlos a inundar el servidor con tráfico.

Señales de un ataque DoS/DDoS:

Rendimiento lento de la red	Sitios web inaccesibles
Servidores inaccesibles	Intentos fallidos de autenticación

Cómo evitar ataques DDoS/DoS:

1) Usa software antivirus en dispositivos personales.
2) Habilita un firewall para protección.
3) Asegura las vulnerabilidades de tus dispositivos en hardware/software.