



Universidad del Caribe

2000

CANCUN, QUINTANA ROO, MEXICO

CONOCIMIENTO Y CULTURA PARA EL DESARROLLO HUMANO

Ingeniería en Datos e Inteligencia Organizacional

Attack Vectors

Profesor:

Ismael Jiménez Sánchez

Alumno:

Chi Huchim Emily Rubi

Tópicos selectos en Ingeniería en Datos

Attack Vectors

Un vector de ataque es una técnica o vía que los actores de amenazas utilizan para acceder o penetrar en una red, sistema, aplicación o dispositivo objetivo. Las amenazas de una organización representan todos los sistemas vulnerables que pueden ser atacados por vectores de amenazas. Los vectores de ataque comunes incluyen credenciales comprometidas, phishing, malware, amenazas internas, vulnerabilidades e inyecciones de SQL. Un actor de amenazas puede utilizar uno o varios vectores de ataque para lograr un objetivo.

Hack Value

Es la noción entre los hackers de que algo vale la pena hacer o es interesante.

Daisy Chaining

Implica obtener acceso a una red y/o computadora y luego usar la misma información para obtener acceso a múltiples redes y computadoras que contienen información deseable.

Exploit

Es una violación de la seguridad de un sistema de TI a través de vulnerabilidades.

Zero-day attack

Es un ataque que explota la vulnerabilidad de la computadora antes de que el ingeniero de software publique un parche.

Vulnerability

Es la existencia de una debilidad (error de diseño o implementación) que puede provocar un evento inesperado que comprometa la seguridad del sistema.