TALENTO TECH

TIC

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 2 – UNIDAD 1

Universidad Tecnológica de Pereira

faceIT

VECTORES DE ATAQUE

Son todos los elementos que pueden convertirse en un punto de entrada para que una persona malintencionada obtenga acceso a un sistema. Entre los diferentes vectores se tiene:

El correo electrónico, a través del cual ciberdelincuentes envían mensajes que parecen legítimos y que pueden lograr que un usuario realice una acción. Por ejemplo, descargar un archivo, exponer un vínculo falso para robar contraseñas o incluso vínculos que descargan e instalan programas con los que atacantes se valen para el robo de información.

Redes inalámbricas gratuitas o abiertas: Este vector de ataque consiste en agentes malintencionados que crean o aprovechan redes abiertas que no piden contraseñas para conectarse. Generalmente aprovechan espacios como aeropuertos, cafeterías, centros comerciales y otros lugares concurridos. Lo que buscan es que usuarios se conecten a las redes abiertas y buscan vulnerabilidades en los equipos conectados. Por ejemplo, si un computador que permite a usuarios anónimos ver los archivos, se conecta a una red abierta, todos los archivos podrán ser leídos por cualquier persona en la misma red. Un atacante fácilmente puede robar información e incluso instalar programas a través de puertos y protocolos no seguros que permitan el acceso desde redes inalámbricas. En esencia, explotar vulnerabilidades por malas **configuraciones de un dispositivo.**

Medios extraíbles: Un vector de ataque son los medios portátiles que se pueden conectar a uno o a muchos computadores. Por ejemplo, CDs, memorias USB, celulares con cables USB, Tarjetas de memoria, entre otros. Un atacante que emplee estos medios suele cargar programas que se ejecutan en cuanto un computador detecte que hay un medio extraíble conectado. Al ejecutar tales programas se crean brechas de seguridad y los atacantes pueden robar información e instalar todo tipo de malware.Se han hallado casos en donde atacantes utilizan memorias con código malintencionado que se dejan en sitios públicos para que alguien las encuentre y las conecte. También a través de regalos gratuitos o incluso atacantes que logran entrar físicamente a donde hay computadores y conectan estas memorias con el fin de robar información.

Exploradores web: Un atacante puede emplear técnicas para confundir a los usuarios y que estos entren a sitios malintencionados. Desde allí se cambian las configuraciones de los exploradores para crear puntos de entrada de los atacantes. También hay sitios que regalan plugins o programas que aumentan las funciones de un explorador, comprometiendo la seguridad en la información. En la imagen se ve un sitio web malintencionado que simula haber hecho un análisis de virus en el computador e intenta engañar al usuario para que entre en un enlace que descarga malware. El engaño consiste en hacer creer que el malware es un programa que eliminará los supuestos virus detectados.

TIC

Servicios en la nube: Los servicios en la nube cuentan con muchas estrategias para interconectar los equipos en la nube, los datos y las soluciones que ofrecen. Generalmente las malas prácticas en la seguridad de las redes y los accesos en servicios de la nube ponen en alto riesgo los datos y comprometen tanto la información como la infraestructura. Por ejemplo, un atacante que logre entrar a un sistema de control de máquinas virtualizadas puede crear decenas o cientos de máquinas y conectarlas a una botnet para atacar. Los servicios en la nube cobran por la capacidad de cómputo instalada por el atacante generando grandes pérdidas económicas.

Agentes internos: Los empleados de las organizaciones pueden actuar como vectores de ciberataques, en ocasiones de forma intencional o en ocasiones con desconocimiento de que son un vector de riego en la seguridad de la información. Un empleado puede ser suplantado y robar información, también puede robar datos intencionalmente y causar daños.