Clase 4:
Actores de amenaza y vectores de ataque

¿Qué es un actor de amenaza *(threat actor)*?

Un actor de amenaza es un individuo o grupo que realiza acciones potencialmente dañinas hacia un sistema de computadoras, red, o entorno digital.

No necesariamente es un "hacker" como se conoce comúnmente, sino que es cualquier persona que cause o quiera causar daño a los sistemas y empresas.

También puede utilizarse el término "atacante".

Actores de amenaza - Atributos

Según sus atributos, los actores de amenaza pueden tener los siguientes atributos o características:

Interno/Externo: de manera interna puede ser cualquier miembro de la organización que rompa sus políticas (con o sin intención); de manera externa puede ser cualquier persona que tenga un fin maligno en mente, desde practicar sus habilidades hasta acabar con la organización por completo, y que no tiene acceso interno de manera directa.

Recursos/Financiación: dependiendo de sus fondos y recursos monetarios, pueden tener equipo de última generación y equipos dedicados a realizar estas actividades, o podría ser una sola persona con simplemente una laptop.

Nivel de sofisticación/Capacidad: depende de las capacidades/habilidades del atacante, y su propio conocimiento para realizar sus actividades delictivas.

Control de entendimiento

¿Un miembro de una organización puede ser un actor de ataque?

Sí

Actores de amenaza - Tipos

Nación-estado: es posiblemente el más sofisticado. Este tipo de atacante tiene a un gobierno entero como patrocinador, por lo que sus recursos de personas, dinero y tiempo son grandes. Pueden ser contratados para atacar otros gobiernos o también empresas.

Amenazas internas (*insider threat*): un empleado que, con o sin intención, generan problemas en la CIA de la organización.

Atacante sin habilidades: no posee mucho talento para realizar ataques, simplemente ejecuta scripts y programas ya creados disponibles públicamente; también se les conoce como "script kiddies" (niños "escripteros").

Hacktivista: personas que utilizan herramientas digitales con intenciones malignas, basados en razones políticas, sociales o ideológicas. Viene de las palabras "hacker" y "activista".

Actores de amenaza - Tipos

Shadow IT: se refiere a recusos tecnológicos (IT) utilizados en la organización sin que esta lo autorice, como instalar software o utilizar hardware que pueda dañar la red y los equipos.

Crimen organizado: grupos de personas que, principalmente con fines monetarios, atacan a personas o empresas utilizando la tecnología. Es sofisticado y cuenta con muchos recursos.

Control de entendimiento

¿Qué tipo de atacante es una persona que ataca a una empresa desde su interior?

Amenazas internas (insider threat)

Control de entendimiento

¿ Qué tipo de actor de amenaza es alguien que toma control de un sitio web de una empresa y cambia su contenido por propaganda religiosa?

Hacktivista

Control de entendimiento

¿Qué tipo de atacantes son dos compañeros de bachillerato que descargan herramientas de internet y ven videos de Youtube para realizar ataques?

Atacantes sin habilidades o script kiddies (niños “escripteros”)

Motivaciones de un atacante

Exfiltración de datos: obtener información sensible de una organización o persona, y removerla, con o sin intención.

Espionaje: obtener información sensible, ya sea para exponerla y afectar a sus clientes, para extorsionar a la víctima, o para utilizarla en otros ataques. Esto se puede lograr tanto física como digitalmente.

Extorsión: aprovechar un ataque o la información obtenida para obtener un beneficio, el cual es monetario en la mayoría de casos.

Interrupción de servicio: causar que los servicios de la organización no funcionen correctamente, intentando lograr que esta pierda dinero y credibilidad.

Beneficio financiero: la mayoría de ataques buscan este fin. El principal objetivo de los ataques de ransomware famosos es obtener ganancias millonarias.

Creencias filosóficas/políticas: pueden haber motivaciones cuyo fin parezca bueno para los atacantes debido a sus creencias.

Motivaciones de un atacante

Éticas: personas cuya ética les indica que algo está bien o mal, y quieren involucrarse realizando ataques para defender sus valores morales.

Venganza: simplemente han sido afectados por una persona o empresa, directa o indirectamente, y quieren afectarla lo más que se pueda.

Alteración/caos: alguien que simplemente quiera causar problemas, sin motivaciones claras más que hacer daño.

Guerra: por motivos de guerra las naciones invierten mucho en tecnología de ciberseguridad ofensiva o subcontratan empresas dedicadas a ello, tanto legales como ilegales.

Nota: las motivaciones dependen de cada persona, por lo que no solamente se queden con las mencionadas acá.

Control de entendimiento

¿El amor puede llevar a un atacante a realizar ataques?

Claro que sí

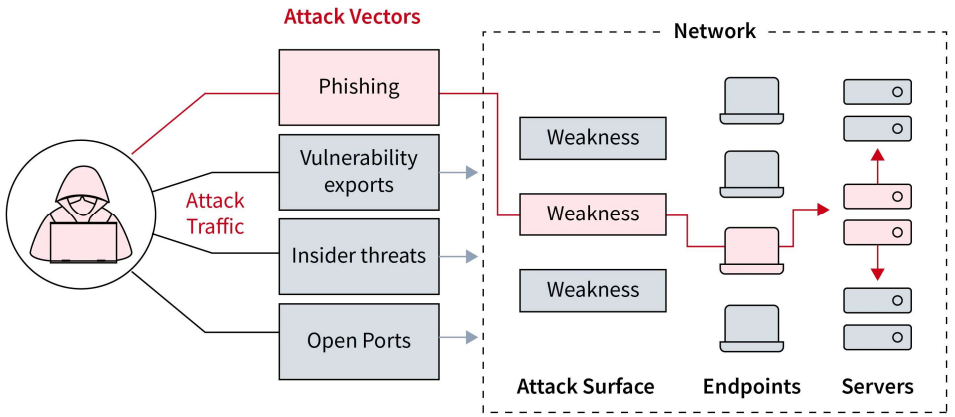
Control de entendimiento

¿Un atacante puede interrumpir servicios por venganza?

Claro que sí

¿Qué es un vector de amenaza *(threat vector)*?

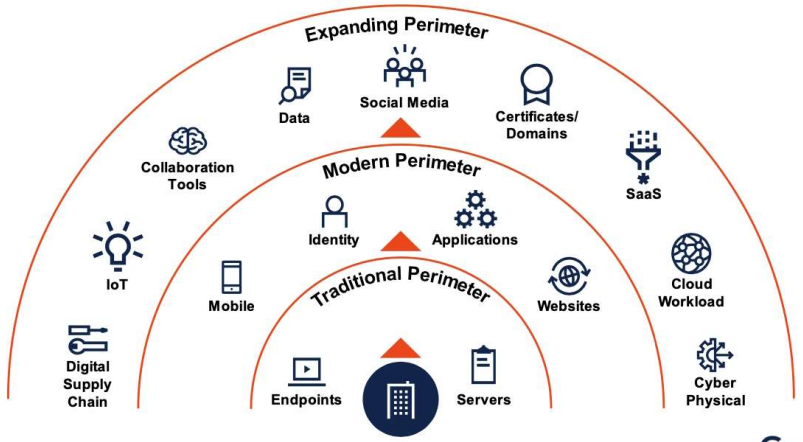
También conocido comúnmente como “vector de ataque”, es el método o camino por medio del cual un atacante puede intentar obtener acceso a un sistema de red.



Los vectores de amenaza se pueden ver como un letrero con varios caminos de los cuales debemos escoger uno a la vez. Es el inicio del camino que se va a tomar.

¿Qué es la superficie de ataque *(attack surface)*?

Se refiere a los posibles puntos o vulnerabilidades, tanto virtuales como físicos, por los cuales un atacante podría obtener acceso a la red interna o extraer información de la misma.
Se puede ver como todos los posibles objetivos de un atacante.



Gartner

Vectores de amenaza y superficies de ataque

Mensajes: se lleva a cabo por medio de métodos de telecomunicaciones, como correos, mensajes instantáneos, u otros parecidos.

Imagen: se pueden crear imágenes para que lleven a cabo ataques cuando estas sean abiertas o procesadas.

Archivo: puede utilizarse cualquier tipo de archivo, como PDFs, ejecutables (.exe), archivos comprimidos, u otros.

Dispositivos extraíbles: son utilizados para introducir malware a los equipos.

Software vulnerable: cualquier software que tenga debilidades y fallas que puedan ser explotadas para realizar acciones no autorizadas.

Sistemas o aplicaciones sin soporte: se refiere a cualquier software que ya no recibe soporte por parte de su fabricante, por lo que pueden surgir vulnerabilidades a lo largo del tiempo.

Vectores de amenaza y superficies de ataque

Redes inseguras: configuraciones faltantes o poco reforzadas pueden facilitar el trabajo de un atacante. Las redes pueden ser cableadas o wireless, como wifi o bluetooth.

Puertos de servicio abiertos: cualquier servicio abierto puede intentar explotarse.

Llamadas de voz: utilizadas para engañar a las personas.

Credenciales predeterminadas: cualquier servicio o herramienta que utilice credenciales por defecto está desprotegido.

Cadena de suministro: cualquier elemento dentro de una cadena de suministro puede ser afectado, causando un mal a todas las partes.

Control de entendimiento

Un atacante accedió a la red interna por medio de un servidor expuesto a internet utilizando SSH.
¿Qué tipo de vector aprovechó el atacante?

Puertos de servicio abiertos

Control de entendimiento

Un atacante obtuvo a la red interna cuando su malware se ejecutó desde la red interna habiendo dejado USBs tiradas cerca de la empresa.
¿Qué tipo de vector aprovechó el atacante?

Dispositivo extraíble

Control de entendimiento

Un atacante obtuvo información privada de clientes al obtener documentos de un distribuidor de paquetes de la empresa.
¿Qué tipo de vector aprovechó el atacante?

Cadena de suministros

¿Qué es la ingeniería social?

Se refiere a un conjunto de técnicas centradas en aprovecharse de las emociones de las personas, como la prisa, familiaridad, poder, miedo...
Se puede usar como mensajes, llamadas, o pláticas físicas.

Vectores humanos/Ingeniería social - Técnicas

El phishing es una técnica que intenta engañar a las personas aprovechándose de sus emociones. Puede presentarse como:

Phishing: envío de correos electrónicos.

Vishing: llamadas de voz.

Smishing: envío de mensajes utilizando mensajería instantánea.

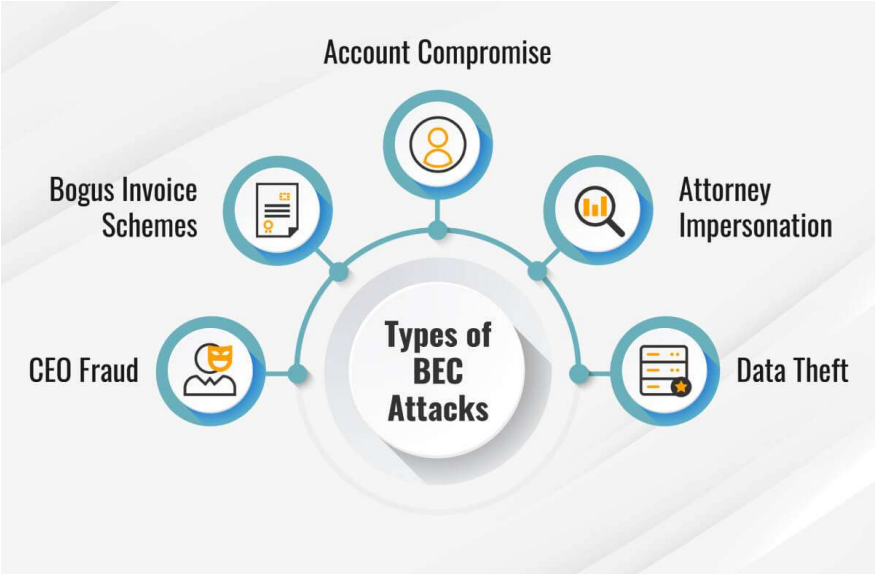
Pueden ir en forma de:

Desinformación: queriendo dejar en mal a una entidad o persona.

Suplantación: hacerse pasar por alguien más para obtener algún beneficio.

Vectores humanos/Ingeniería social – Técnicas específicas

Compromiso de correo de negocios (Business Email Compromise, BEC): utilización del phishing para hacerse pasar por alguien de la organización víctima, utilizando el formato de correos y nombres propios de los empleados de esta.
Pueden hacerse pasar por jefes, equipo de TI, equipo de finanzas, u otros dependiendo del fin que el atacante tenga en mente.



Vectores humanos/Ingeniería social – Técnicas específicas

Pretexting: técnica de ingeniería social utilizada cuando se quiere engañar a una víctima de manera física. En esta técnica se prepara una identidad falsa (un pretexto), imagen y vestimenta cercanos a los utilizados en las organizaciones, y se preparan contactos que también se hagan pasar como superiores en caso de que se deba llamar a alguien.
Se preparan también elementos como gafetes, documentos, uniformes, u otras cosas que ayuden a acercarse a algo real.
El objetivo principal es obtener información o acceso.

Vectores humanos/Ingeniería social – Suplantación de marca

Existen ataques o técnicas que intentan hacerse pasar por una marca u organización, con el fin de desprestigiar u obtener información:

Charco de agua (Watering hole): se obtiene control de un sitio web bastante utilizado (como un charco de agua en la selva) y se cambia su contenido para mostrar u obtener información. El objetivo es afectar a la mayor cantidad de personas.

Typosquatting (secuestro de URL): técnica en la cual se crea uno o varios dominios cuyo nombre sea parecido al de la empresa víctima, pero cambiando caracteres, como grnail.com o gmai1.com en lugar de gmail.com.

Vector de amenaza y superficie de ataque

Ejemplo 1

Vector de amenaza: correo de phishing
Parte de la superficie de ataque objetivo: empleados poco preparados contra phishing.

Ejemplo 2

Vector de amenaza: vulnerabilidades en sitio web
Parte de la superficie de ataque objetivo: sitios web de la empresa que presenten vulnerabilidades.

Control de entendimiento

En el compromiso de correo empresarial se crean dominios con el nombre parecido al de la empresa.

Falso – Eso es typosquatting

Control de entendimiento

El pretexting es una técnica que utiliza interacciones físicas para engañar a las personas.

Verdadero

Lectura asignada

A partir de la lectura de las **páginas de la 8 a la 11** (capítulo *"¿Qué es el phishing?"*) del libro "*Ciberseguridad para niños con Minecraft*", responda la siguiente pregunta en el foro de Sinapsis utilizando sus propias palabras:

¿Qué consejo se da para confirmar información proveniente de campañas de phising?