Ciberataques

Transcribed on July 5, 2025 at 10:58 AM by Minutes AI

Speaker 1 (00:02)

Esta nueva sesión donde vamos a trabajar los conceptos, algunos tipos de ataques, algunos tipos de amenazas.

Vamos a ampliar un poco el conocimiento expuesto en otras sesiones.

Como digo, vamos a empezar hablando de algunos tipos de ataques, tenemos que conocer cuáles son los ataques que nos pueden realizar contra normativación, contra estos activos y luego además profundizaremos a través de conceptos básicos, hablaremos de amenazas, iremos clasificando un poco y definiendo todos estos tipos de conceptos.

Empezamos hablando de ataques malware, son comúnmente conocidos, hay diferentes tipos de malware, hay diferentes tipos de infecciones.

Cada malware o cada tipo de malware se puede hacer diferentes tipos de acciones sobre un sistema y al final son grandes amenazas a las que se enfrentan las organizaciones.

El malware se puede clasificar de diferentes tipos, tenemos troyanos, tenemos virus como tal, tenemos ransomware, tenemos spyware, diferentes tipos de malware, cada uno con funcionalidades diferentes, con objetivos diferentes.

Pero hoy en día sobre todo los temas de ransomware son bastante críticos porque afectan a las empresas, porque secuestran información de las organizaciones, secuestran, cifran documentos importantes de las organizaciones y piden un rescate por ello.

Generalmente empresas grandes puede no tener un impacto, no tener un impacto muy grande porque es verdad que la contramedida, la mitigación, puede ir asociado a un plan, tener sus copias de respaldo, aislar la amenaza y restaurar y perder unas horas de trabajo casos en los que puede ser bastante crítico para la operación, para la actividad de negocio de la oferta pyme, es decir, el no tener acceso a información importante de la empresa, ya sea de clientes, contabilidad, etc, pues puede provocar incluso la desaparición de la prueba pyme si no tienen sus planes de mitigación, en este caso sus planes de copia de respaldo.

Bueno, el tema de las infecciones de malware son ataques a los que se enfrentan las organizaciones, están ahí desde hace ya décadas, existe desde hace décadas y es algo que tenemos que tener en cuenta.

También tenemos ataques de ingeniería social, por ejemplo las campañas de phishing, que son quizás el símbolo más más conocido que tiene la ingeniería social, pero los ataques de ingeniería social lo que afecta es el componente humano que tiene toda la organización, es decir, al final la actividad de negocio la van a realizar personas que tienen sus vidas, que tienen sus conocimientos y estas personas al final pueden ser el blanco de ataques de ingeniería social en el cual se les presenta o se les intenta presentar algún tipo de mundo que parece real pero no lo es y hacer que confíen en los atacantes para realizar algún tipo de acción.

Lo más común o lo más normal, lo más conocido son las campañas de phishing, donde al final recibimos un email que puede parecer o nos pueden engañar, desde ese email pasamos a una página donde nos están solicitando unas credenciales, algo que identificamos como que puede ser parte de la empresa o algo con lo que la empresa se sienta cómodo, o identificamos como que es algo que conocemos y a partir de ahí nos roben credenciales, nos roben información, nos pidan datos y como usuarios de Internet también incluso tarjetas de crédito que puedan solicitarnos, etc.

Bien, esos ataques de ingeniería social han ido evolucionando, es decir, no se quedan solamente en un correo electrónico que nos hacen llegar, en un entorno con la página web que nos hacen, que nos muestran, sino que ha ido evolucionando con la llegada de los dispositivos móviles, posteriormente con tecnologías como Auth y con tecnologías como la inteligencia artificial, donde ya el tema de acumulación de voces o la acumulación incluso de imágenes que pueden presentarnos a una persona como una deepfake, a una persona como si fuera real lo que estamos viendo y no lo estamos viendo realmente, o una voz que nos habla, que realmente identificamos con una persona y que realmente está generada por una IA, pues ese tipo de evolución también es ingeniería social y es una amenaza, es una amenaza a la que nos enfrentamos como sociedad y las empresas también se enfrentan a ellas.

Comentar también sobre la ingeniería social, bueno, aparte que se verá en un módulo, comentaros en esa evolución, hay un caso muy particular que es la estafa del CEO.

La estafa del CEO es una de las amenazas a las que se enfrentan las empresas muy particularmente, porque es un tipo de phishing en el cual se hace llegar un correo electrónico haciéndose pasar por el CEO de la empresa o por alguien importante en la empresa que tiene el poder para solicitar pagos urgentemente y si el agente de contabilidad pues cae ante ese tipo de bueno, confía en ese correo porque lo envía el CEO, pues incluso pueden llegar a hacer operaciones de lo que se le solicita en ese correo electrónico.

Claro, eso ha evolucionado también, como decía, a través de la inteligencia artificial y tenemos casos en los que hablamos de que te llaman videollamada, encuentras una persona a otro lado que es CEO o alguien que tú identificas tu organización con el poder para decirte esto, o una llamada de Skype, de Teams o de otra plataforma, una llamada

Entonces, bueno, son ataques que han ido evolucionando.

Como veis, hay un modelo muy clásico que es el phishing en biomasa.

Hay algún tipo de phishing malo en el cual había muchos detalles muy fácilmente detectables.

Eso ha ido evolucionando y cada vez perfeccionan más este tipo de avenado.

Bien, también tenemos como ataques de delegación de servicio, ordenación de servicio distribuido.

La denegación de servicio consiste, bueno, afecta totalmente a la disponibilidad, como hablábamos en la parte de seguridad de información, la dimensión de confidencialidad, disponibilidad e integridad.

Los ataques de dos o ddos pues afectan totalmente o directamente a la parte de disponibilidad de la información.

Entonces un ataque DBS puede afectar a un servicio de memorización o puede afectar a muchos servicios o puede incluso colapsar la operativa en Internet.

Si imaginamos que tenemos una tienda virtual, donde mi empresa es una tienda virtual en Internet y de repente sufre un ataque de servicio, ya sea simple, distribuido, pues mi operativa se cae a cero, mi negocio cae a cero, se queda fuera de Internet, queda no disponible y mi actividad de negocio cae literalmente a cero, no puedo operar.

Entonces es algo crítico.

Por supuesto existen soluciones o protecciones para este tipo de ataques anti DDs, también en la parte hackingético que nos permite medir cómo funcionan o como eficientes son los controles o las inversiones en seguridad que estamos haciendo en la organización, pues ahí tenemos la posibilidad de medir si las soluciones o la inversión en seguridad, el anti DDOs de turno que tengamos contratado, pues está siendo eficiente y está siendo eficaz.

Sobre todo son pruebas que dan miedo probar, es decir, en un jarquinético, pero que son a veces importantes.

La amenaza en sí, el dos o DDOs, es que nos podemos quedar fuera o primer negocio se puede quedar fuera de la operativa, eso es algo bastante crítico, dependiendo también de la naturaleza de la empresa.

Más tipos de ataques, bueno, tenemos los de inyección, yo he puesto aquí Cobalt Injection, pero esto es a nivel global, son inyecciones, son ataques muy comunes, ya sean por SQL injection, no SQL injection, Lrap injection, vulnerabilidades al final de inyección, ejecución de comandos, hay muchos tipos que se pueden agrupar.

Al final pues las vulnerabilidades al final son vulnerabilidades que podemos tener en el software, ya sea un software de terceros o ya sea nuestro propio software desarrollado por nosotros, pero podemos tener vulnerabilidades.

Entonces al final son amenazas, vías de ataque que tienen los delincuentes o atacantes para poner en jaque nuestra nuestra seguridad.

Entonces bueno, con Injection es una de las posibles vías, agrupa muchos tipos de vulnerabilidades, por eso lo he colocado aquí y al final es uno de los ataques o de las vías de ataque que también se ve bastante.

Luego también tenemos la fuerza bruta, que como concepto, como concepto, la fuerza bruta lo que nos aporta es o la podemos definir como el proceso por el cual se se van probando contraseñas hasta que se da con la contraseña correcta para un usuario.

Entonces, lógicamente nosotros tendremos sistemas en los cuales podemos detectar que están haciendo ese tipo de fuerza bruta, que están haciendo ese tipo de pruebas, banear conexiones y poner algunas reglas para que esas direcciones IP que nos están haciendo esa fuerza bruta no queden baneadas y no nos puedan seguir haciendo ese proceso.

La fuerza bruta final es un ataque en el cual si tenemos una mala configuración, una mala política contraseña, pues puede que los usuarios de la organización utilicen contraseñas que son fácilmente adivinables porque se encuentran en diccionarios, porque se pueden generar de manera sencilla, porque son palabras muy utilizadas.

Cada año sale un ranking de las 25, de las 50, de las 100 contraseñas más utilizadas.

Pues lógicamente tenemos que tener este tipo de cosas en cuenta.

En el momento que ponemos una complejidad suficiente a la contraseña, donde tengamos que meterle cá mayúsculas, minúsculas, números alfanuméricos, tres especiales, 1 longitud grande, pues estamos rebajando esa capacidad de fuerza bruta.

Pero sobre todo cuando metemos 1 s factor autenticación es cuando ya estamos haciendo que la fuerza bruta no tenga ya sentido.

Porque una cosa es averiguar una contraseña, pero si luego hay 1 s factor de autenticación que pasar, entonces el tema se nos complica.

Luego la fuerza bruta se puede aplicar o generalmente si tenemos servicios estándares, en puertos estándares, por ejemplo ssh, el FTP y lo tenemos en puertos estándar.

El ssh, si yo tengo un ssh, quizá no debería tener autenticación por usuario y contraseña, tendría que tenerlo por clave pública, pero además tendría que tenerlo en un puerto no estándar, no en el 22.

De manera que si quieres encontrar mi ssh tendrás que identificarlo en un puerto alto.

Eso ya rebaja también las posibilidades.

Pero bueno, tenemos que conocer las amenazas, tenemos que conocer los ataques y la fuerza bruta al final es un proceso que sigue funcionando por desgracia hoy en día y que sobre todo en entornos, por ejemplo, director activo, son entornos más internos, los usuarios, dependiendo la política que tengan de complejidad de contraseña, etc.

Pero bueno, puede ser que también otro entorno que se pueda aplicar.

También contar que la fuerza bruta luego tiene algunos derivados interesantes, por ejemplo el password spriting, que al final es un tipo de fuerza bruta, porque al final no fijamos un usuario y probamos contraseñas, sino lo que hacemos es fijar una contraseña y probamos usuarios, es decir, esta contraseña está entre las 100 más utilizadas del mundo, a ver si algún usuario de tu organización la tiene.

Entonces claro, ahí está el tema.

Es justo contrario a lo que hemos definido como fuerza bruta, pero es un tipo de fuerza bruta, lo que es el password.

Fijamos un password y probamos en esos usuarios, por ejemplo, en entorno director activo, si tienes el listado de usuarios de director activo, tú puedes fijar una contraseña y ver si alguno de esos usuarios tiene mecanismos que desde el punto de vista genético se van a utilizar, pero también, por supuesto, los atacantes externos también van a utilizar, con lo cual debemos intentar eliminar la posibilidad de en alguno de nuestros servicios de la organización.

Luego tenemos otro tipo de ataque, otro conjunto de ataques que son los de mining middle, que no es solamente un tipo de ataque sino una categoría donde tenemos diferentes formas o existen diferentes formas de hacer Mindy middle.

Al final el concepto de Mindy Middle es colocar un equipo en medio de una comunicación.

Existen varias formas, entonces iréis viendo algunas en la formación.

El concepto es este, colocar en medio de una comunicación una máquina con el objetivo de poder observar esa información, esa comunicación, incluso en algún momento puede incluso hasta manipularla, ya sea porque inyectamos un certificado o ya sea porque se modifica el tráfico que va en texto plano, se puede modificar, se puede modificar ficheros, se puede modificar todo porque está pasando por medio de el atacante está colocado en medio de la comunidad, no solamente puede visualizar esa comunicación, esa información que se intercambia en dos máquinas, sino que podría incluso hasta modificarla.

Son ataques a los cuales lógicamente estamos expuestos.

Por supuesto, canales seguros, empezamos a evitar este tipo de ataques de Mind the middle.

Si nos puede inyectar un certificado, que podemos tener una cadena de certificados pineada en la comunicación y bueno, podemos tener diferentes mecanismos, podemos tener también el propio cifrado punto a punto entre dos máquinas, tenemos mecanismos también para proteger de este tipo de ataques.

El último tipo de ataque amenaza que vamos a ver en esta slide, pues es el de explotación de memoria.

Al final esto son vulnerabilidades, aplicaciones también son vulnerables, aplicaciones, por ejemplo, buffer overflow, el se overflow, diferentes tipos de overflow pueden afectar a diferentes aplicaciones que se codifican de una manera incorrecta, que se introducen este tipo de vulnerabilidades y que pueden ser explotadas a través, por ejemplo, de un exploit.

Al final un exploit no es más que una aplicación que sabe cómo poder aprovecharse de una vulnerabilidad de un software, una versión concreta.

Entonces es un tipo de ataque también que si tenemos un servicio expuesto que se conoce que hay una vulnerabilidad de tipo buffer overflow o stack buffer overflow, pues tenemos que lógicamente, o aislar ese servicio, mitigar o actualizar si existe alguna actualización, pero tenemos que al menos aislar ese servicio y poder solventar o poner protecciones alrededor para poder detectar si me va a intentar lanzar el spread contra mi servicio, etc.

En ese ejemplo tendríamos que buscar esas soluciones, pero son un tipo de ataque también que no vamos a encontrar mucho.

Ahora vamos a ver algunos conceptos básicos, he juntado aquí algunos que nos tienen que sonar de cada formación, después de la formación también.

Y vamos a empezar hablando de APT Advanced Persistence, Amenaza persistente avanzada.

Esto es un tipo de ataque en el cual por definición se requiere mucho tiempo y muchos recursos porque son ataques un poco más avanzados de lo normal.

Entonces estos son ataques que no están al alcance de cualquiera, tienen unos objetivos muy complejos y muy difíciles y pues involucra generalmente se involucra muchas veces el estudio de alguna vulnerabilidad de tipo day donde no se conozca, que no sea una vulnerabilidad conocida y bueno, pues ya como digo, requiere bastante complejidad.

Al final el objetivo es lograr, por la parte de los atacantes, lograr el acceso al sistema o a los sistemas o los dispositivos y lograr una cierta persistencia para lograr sus objetivos que tengan ellos.

El apt tiene su parte en el hacking ético también como una prueba, es decir, básicamente en el hacking ético se hace todo de manera legal, que es lo que a nosotros nos interesa en esta formación, lógicamente.

Y en la parte de simulación de apt lo que se busca es un poco, se contrata ese servicio para buscar cómo un equipo de pentesters en este caso, puede lograr el objetivo que se plantea, por ejemplo, el objetivo que se plantea que por ejemplo puede ser lograr acceso al dispositivo móvil de del CEO de la empresa o del CiSO de la empresa, lógicamente contratan el servicio para hacer esa prueba y es un reto bastante grande.

Es un ejemplo.

Luego tenemos como concepto el de data leaks, el de fuga de datos.

Esto es un brechaz de datos.

Al final una empresa tiene una vulnerabilidad o ya se puede ser también un insider dentro del acceso a la información.

Sea como sea, sale esa información, que suelen ser bases de datos con identidades digitales o información propia de la organización, sale fuera de la empresa y es publicada, muchas veces es publicada, en algunos casos es vendido también.

Entonces un data leak va en torno a este concepto.

Luego tenemos el phishing, que ya lo hemos explicado como concepto.

Tenemos también la actualización de software, importantísimo, los sistemas deben estar actualizados porque al final no está actualizado supone tener vulnerabilidades y hoy en día con las fuentes de información que existen en Internet como security focus, exploitv, day to day, al final existen muchas fuentes de información donde tenemos muchas vulnerabilidades publicadas, tenemos exploit y tener sistemas no actualizados puede provocar que tengamos una seguridad baja en este entorno.

Tenemos el concepto de ransomware.

También se ha aplicado antes, con lo cual vamos a pasar al siguiente.

El exploit también se ha aplicado, acordaros, aplicación que implementa cómo aprovecharse una vulnerabilidad.

¿Con el objetivo de qué?

De ejecutar código.

Ese código al final proporcionará el control de esa máquina a un atacante y si estamos en el ámbito hacking ético, pues a un pentester, que es el ámbito que nos interesa del hacking ético.

Tenemos el concepto de zero day.

El concepto de zero day es el concepto en el cual existe una vulnerabilidad, un cero day, y no hay solución para ello, no hay parche, no hay actualización, por lo cual tenemos un problema.

Tendremos que aislar ese servicio o esa aplicación que es vulnerable de forma que no se le pueda interactuar directamente con ella.

Si no podemos quitarla porque es algo fundamental en nuestra actividad de negocio, necesitaremos poner alguna protección, IDs, IPs, algo que podamos detectar que nos estén enviando ese payload malicioso hacia el servicio vulnerable.

Tendremos que jugar un poco con ello.

Luego tenemos el concepto del bug bounty.

El concepto de bug bounty es un programa donde recompensas, es decir, las empresas quieren auditar una serie de sitios web o una serie de dominios, una serie de algo que es de ellos, ponen unas reglas, ponen unas reglas e invitan a la gente a Oye, pues audítame, hazme un jardín kinético, pero solamente buscando ciertos tipos de vulnerabilidades que están en las reglas.

Además, hay que cumplir muy bien las reglas que ellos marcan, porque ahí están en línea roja.

Es decir, si nos pasamos y hacemos algo que no está en esas reglas del juego, estaremos seguramente cometiendo un delito.

O sea, que hay que fijarse bien en las reglas que se marcan en un Bug Bounty y además en qué vulnerabilidades están interesadas estas empresas, porque en el momento que se encuentren se reportan a la empresa siguiendo el programa de Bubonti.

Y hay una serie de premios, la empresa tiene como una serie de premios donde se paga un dinero por esas vulnerabilidades que ellos han indicado que se están buscando, sobre los activos que se están buscando.

Es importantísimo.

Luego tenemos el concepto de SSDLC, que es el ciclo de vida desarrollo seguro.

Esto es algo importante que también entra en juego con el concepto del devsecops.

El SSDLC es el ciclo de vida y desarrollo de una aplicación.

Ya puede ser una metodología clásica o una metodología Yale de hoy en día, pero lo que hacemos es que en cada fase del desarrollo se introducen pruebas de seguridad, se van metiendo pruebas de seguridad que van haciendo que pensemos en la seguridad desde el principio.

Desde que concebimos el sistema que vamos a desarrollar estamos pensando en la seguridad de este, de forma que estamos haciendo que el sistema resultante, cuando acabemos la parte de desarrollo, las pruebas y pongamos en producción el sistema, el sistema es mucho más seguro que lo que sería si no hubiésemos tenido en cuenta las pruebas de seguridad desde el principio.

El concepto de ciclo de vida de desarrollo y tenemos también el concepto de Devsecops, que es la evolución del DevOps.

Y en el DevOps tenemos a la gente que desarrolla unida en un flujo con agente de operaciones, van integrados y ahora metemos la parte de seguridad en cada fase del DevOps, de forma que va alineado todo y no se concibe de forma aislada.

Como conclusiones hemos estado viendo tipos de ataques, tipos amenazas, hemos hablado de ingeniería social, hemos hablado de malware, hemos hablado de servicio, de explotación de vulnerabilidades, de mejora bruta de las comunicaciones.

Hemos visto un poco un repaso global de los tipos de ataques y amenazas más comunes a nivel general.

Lógicamente si hablamos de malware o si hablamos luego de Mindy Middle o hablamos de vulnerabilidades, podemos desglosarlo muchísimo más, pero estamos hablando en un primer estazo global.

Y luego por último hemos hablado de conceptos básicos, un repaso de conceptos básicos que en el momento que vayan saliendo durante la formación os tienen que que sonar.

Recordar que todo lo que se enseña es desde el punto de vista ético, que es a nivel formativo y educación y que no nos hacemos responsables de ningún mal uso de toda esta información que se vaya a dar.

Bien, pues llegamos al final de esta sesión.

Nos vemos en la siguiente sesión.