UD2 LAB1 - CLASIFICACIÓN DE INCIDENTES DE CIBERSEGURIDAD

ATAQUE 1:

Una tienda en línea sufre un ataque DDoS durante el Black Friday. Un grupo de atacantes usa una red de bots para inundar los servidores del sitio web con tráfico, haciendo que los usuarios legítimos no puedan acceder y realizar compras, lo que resulta en pérdidas económicas significativas.

TIPO DE INCIDENTE

- Este ataque es un ataque DDoS (Ataque de denegación de servicio distribuida)
- Este ataque es muy común entre los ciber delincuentes. Estos usan ordenadores de gente inocente que han caído en trampas ya sea abrir una web, descargar un archivo desconocido o simplemente presionando donde no debían. Cuando el delincuente hace este ataque, a través de un malware que tienen estos PC de inocentes envían peticiones a la web atacada de tal manera que el servidor de esta web se sature.

MODELO CIA

- En cuanto a la confidencialidad de los datos, este ataque no representa una amenaza a la hora de robar datos ya que simplemente este ataque se utiliza para saturar servidores
- Sobre la integridad de los datos, no compromete ni la exactitud ni la consistencia ya que estos datos no están siendo manipulados en ningún momento
- Por ultimo lo que si que hace este ataque es impedir el acceso a los sistemas y también al servicio que esta empresa ofrece. Los atacantes pueden pedir un

monto de dinero a cambio de que dejen de mandar peticiones y dejen de explotar los servidores con ordenadores de inocentes

ORIGEN DEL INCIDENTE

- El ataque es externo es decir viene desde fuera de la organización. Estos ciberdelincuentes se encargan de tener una red de ordenadores inmensa para que cuando ellos quieran, realicen un ataque para dejar sin servicio a los servidores.
- Estos bots como ya he dicho antes, suelen ser creados por personas inocentes que pinchan a links o descargan cosas malignas y no se enteran de que están descargando un software malicioso que corre cuando los ciberdelincuentes quieran

NIVEL DE CRITICIDAD

- El ataque puede resultar en pérdidas económicas significativas, especialmente durante un evento crítico de ventas como el Black Friday, afectando la reputación de la organización y su capacidad de generar ingresos. Por lo cual el nivel de gravedad es alto si no se soluciona a tiempo

ATAQUE 2:

Un empleado descarga un archivo adjunto de correo electrónico aparentemente legítimo, que contiene un troyano. El troyano se instala en el equipo del empleado y permite a los atacantes robar credenciales, exfiltrar datos y espiar las comunicaciones de la empresa.

TIPO DE INCIDENTE

- Este incidente es un caso bastante peligroso. Se trata de un troyano.
- Este malware, se encarga de robar lo que el ciberdelincuente quiera. E incluso a través de técnicas poder llegar a puestos mas altos con información confidencial y de gran utilidad para el ciberdelincuente

MODELO CIA

- En cuanto a la confidencialidad, este ataque si que afecta a la seguridad de los datos, se trata de un software que el trabajador no sabe que tiene en su equipo y se encarga de robar, cifrar o utilizar esos datos para fines malignos
- Esto también afecta a la integridad de los datos, el atacante dependiendo de los permisos del trabajador, puede editar datos o simplemente eliminarlos y quedarselos para utilizarlos. Ademas este atacante puede utilizar técnicas para poder escalar permisos hasta llegar a usuarios que contengan datos mas importantes.
- Este ataque puede impedir el acceso a los sistemas y servicios ya que existen troyanos que hagan que el delincuente tenga el control del sistema de tal manera que también pueda bloquear la entrada a los trabajadores. Es decir que alteren sistemas críticos del sistema

ORIGEN DEL INCIDENTE

- El ataque es interno. El trabajador puede haber recibido un email que pareciese legítimo y haber pinchado en el y sin que se diese cuenta haber instalado un troyano. O a la hora de instalar una herramienta, este no sabe si a parte de la herramienta, te viene un troyano incluido que no sale en la instalación.

NIVEL DE CRITICIDAD

- Este ataque tiene un nivel muy alto de criticidad, ya que el atacante con el control del ordenador de una organización, puede obtener bastante información que posteriormente podría ser utilizada para fines no éticos.

ATAQUE 3:

Un grupo de empleados recibe correos electrónicos que parecen ser de su banco, pidiendo que "actualicen" la información de sus cuentas. Uno de ellos cae en la trampa y proporciona las credenciales de acceso, lo que permite al atacante acceder a la cuenta de la empresa y robar información bancaria.

TIPO DE INCIDENTE

- Este incidente se trata de un ataque de phishing.
- El atacante trata de engañar a un grupo grande de empleados con un correo que parece legítimo y al caer uno de ellos y poner las credenciales, el atacante con esas credenciales podría conectarse de manera remota al servidor o simplemente robar datos de este trabajador.

MODELO CIA

- En cuanto a la confidencialidad, este ataque de phishing lo que hace es robar usuario y contraseña de un usuario o mas por lo cual los datos corren peligro si el ciberdelincuente sabe moverse bien
- Esto puede afectar también a la integridad de los datos dependiendo de los permisos que tenga el trabajador. Con el usuario y contraseña, el delincuente puede modificar datos que el trabajador tenga permitido modificar.
- Este ataque hay muy pocas probabilidades de que afecte a los sistemas y servidores a menos que el trabajador atacado tenga los suficientes permisos para utilizar herramientas de servidor.

ORIGEN DEL INCIDENTE

- El origen del ataque es tanto externo como interno. Es externo ya que el delincuente ha preparado una cantidad de emails para enviar a los trabajadores e interno ya que estos trabajadores son los encargados de saber a que links entran y donde ponen sus credenciales.
- Es necesario que las empresas tengan una formación para sus trabajadores de tal manera que no puedan surgir estos casos ya que algunos emails pueden ser fáciles de detectar pero aun así siguen cayendo.

NIVEL DE CRITICIDAD

- El nivel de criticidad es alto. Cualquier ataque que suponga un robo de credenciales, supone un gran peligro para la empresa ya que este ataque se encarga de utilizar estos datos para robar información o utilizar esa misma información para diferentes cosas.

ATAQUE 4:

Una organización descubre que un atacante ha robado una base de datos de clientes, que incluye nombres, direcciones de correo electrónico y números de tarjetas de crédito. Esta información fue exfiltrada a través de una vulnerabilidad en el software de la empresa, y los datos ahora están disponibles en la dark web

TIPO DE INCIDENTE

- Este ataque es una exfiltración de datos.
- Al parecer se ha robado un montón de información que pertenecía a una base de datos que tenía vulnerabilidades que no se sabía que tenia esta base de datos y que un ciberdelincuente se ha sabido aprovechar

MODELO CIA

- Este incidente es muy peligroso. Afecta totalmente a la confidencialidad de los datos que han sido robados de esa base de datos y que después se han filtrado por la dark web haciendo que todo usuario que acceda a esta y necesite los datos, los pueda obtener de manera sencilla y sea información bancaria o datos personales de los clientes.
- Esto puede afectar a la integridad de los datos. Los usuarios de la dark web que no son pocos, pueden utilizar estos datos y modificarlos de cualquier manera y no con fines éticos
- Esto no afecta a la disponibilidad de los clientes pero este robo de datos puede hacer que la empresa necesite modificar x información y cambiar por completo la base de datos comprometida

ORIGEN DEL INCIDENTE

- El origen del incidente es externo aunque también puede ser interno. Los atacantes han sabido aprovechar una vulnerabilidad de la seguridad de la base de datos. Pero esa seguridad se encarga de formalizarla la empresa que no ha tenido en cuenta esa vulnerabilidad explotada por el ciber delincuente.

NIVEL DE CRITICIDAD

- El nivel de criticidad de este ataque es bastante alto. Los datos robados son una parte muy importante de una empresa y deberían de estar lo mas seguros

posibles para evitar problemas legales además de influir en la reputación de la empresa. Con lo cual es imprescindible tener un nivel de seguridad bastante alto en las bases de datos.

ATAQUE 5:

Un atacante llama al departamento de soporte técnico de una empresa haciéndose pasar por un empleado y logra engañar a un miembro del equipo para que le revele la contraseña de administrador. Usando esta contraseña, el atacante accede al sistema de la empresa y roba datos sensibles.

TIPO DE INCIDENTE

- Este ataque es un ataque de ingeniería social
- El delincuente se hace pasar por un empleado para poder acceder a las contraseñas de administrador y así poder tener control total de los servicios de la empresa y poder obtener información confidencial

MODELO CIA

- En cuanto a la confidencialidad, esta se ve comprometida ya que ha habido un robo de datos por parte de alguien no autorizado y se puede robar información de la empresa
- Al igual que la confidencialidad, este delincuente al tener la contraseña de administrador, a parte de robar datos puede también modificarlos de tal manera que incluso la propia empresa se quede sin acceso a estos
- Este ataque podría afectar a la disponibilidad debido a que el atacante podría tener acceso a servicios y podría utilizarlos para quitar disponibilidad a clientes de la empresa

ORIGEN DEL INCIDENTE

- El origen del incidente es interno ya que el propio trabajador cayó en la trampa del atacante al proporcionar la contraseña de administrador a alguien no autorizado. Es importante que la contraseña de administrador la tenga la menos gente posible y nunca se de alguien si no es en persona

NIVEL DE CRITICIDAD

- El nivel de criticidad es alto. La obtención de credenciales de administrador y el acceso a datos sensibles representan un riesgo significativo para la seguridad de la organización, lo que podría tener repercusiones legales y de reputación.

ATAQUE 6:

Un equipo de seguridad de una empresa detecta que un atacante ha estado realizando un escaneo de puertos en su servidor web. El análisis revela que uno de los puertos está abierto y vulnerable debido a la falta de actualizaciones de seguridad en el software del servidor.

TIPO DE INCIDENTE

- Es un escaneo de puertos
- El atacante ha hecho un escaneo de puertos y el equipo de seguridad ha detectado que lo estaba haciendo. Gracias a eso han podido descubrir una vulnerabilidad que el atacante no ha explotado por lo cual se podría corregir

MODELO CIA

- Este incidente podría afectar a la confidencialidad de los datos solo si el atacante haya podido explotar dicha vulnerabilidad. Pero no lo ha hecho por lo cual no afecta directamente.
- Este incidente hasta que no se explota la vulnerabilidad no afectaría a la integridad de los datos
- Como ya se ha dicho, el atacante solo ha realizado un escaneo de puertos por lo cual ningún servicio estaría comprometido a menos que el atacante utilizase esa vulnerabilidad para aprovecharse

ORIGEN DEL INCIDENTE

- El origen del incidente es externo ya que ha sido el atacante quien ha decidido hacer un escaneo de puertos a la ip de la empresa aunque no haya hecho nada mas que eso.

NIVEL DE CRITICIDAD

- El nivel de criticidad es medio ya que el atacante solo hizo un escaneo de puertos. El problema sería si el atacante decide explotar la vulnerabilidad encontrada de forma maligna. De todas formas esto ayuda a la empresa a corregir esa vulnerabilidad así que en parte es bueno el escaneo.

ATAQUE 7:

Un atacante utiliza un script automatizado para intentar acceder a una cuenta de administrador en un sistema de la empresa. Tras múltiples intentos fallidos, logra adivinar la contraseña y obtiene acceso no autorizado, comprometiendo información confidencial.

TIPO DE INCIDENTE

- Se trata de un ataque de fuerza bruta
- Estos ataques son bastante típicos a la hora de entrar a un sistema donde no se conocen las credenciales. Normalmente los ciber delincuentes los suelen utilizar en sistemas que no puedan reconocer que se esta realizando un ataque de fuerza bruta.
- Consiste en mediante una herramienta, probar miles de combinaciones en las credenciales hasta que salga la correcta. Se suelen utilizar diccionarios de claves para este tipo de ataques que pueden ocupar gigas llenas de palabras

MODELO CIA

- Este incidente afecta directamente a la confidencialidad de los datos ya que el delincuente ha probado muchas maneras para entrar y robar estos datos y utilizarlos
- También puede perfectamente modificar datos de modo que también afectaría a la integridad de estos

- A menos que el atacante utilice herramientas para bloquear el acceso, la disponibilidad no debería de verse comprometida. Esto ya depende del atacante y lo que hará dentro del sistema

ORIGEN DEL INCIDENTE

- El origen del ataque es totalmente externo. El personal de la empresa no tiene nada que ver con el ataque. El atacante ha utilizado un ataque de fuerza bruta para poder acceder al sistema con sus herramientas.

NIVEL DE CRITICIDAD

- El nivel de criticidad de este ataque es bastante alto ya que una persona no autorizada dentro de un sistema, puede hacer lo que quiera. El atacante simplemente utiliza distintas herramientas para acceder a este

ATAQUE 8:

Un atacante explota una vulnerabilidad de día cero en el sistema operativo de una empresa, lo que le permite ejecutar código malicioso en los servidores y tomar control del sistema. La empresa no había aplicado las actualizaciones de seguridad necesarias, lo que permitió el ataque.

TIPO DE INCIDENTE

- El ataque es una explotación de una vulnerabilidad de día cero
- El atacante ha dado con una vulnerabilidad que es posible explotarse de tal manera que lo ha hecho y esto le permite ejecutar código y hacer prácticamente lo que quiera dentro del sistema

MODELO CIA

- En cuanto a la confidencialidad, supone un grave problema ya que el atacante puede ejecutar código para poder visualizar archivos confidenciales y utilizarlos
- El atacante al poder ejecutar código malicioso, también puede modificar los datos del sistema por lo cual también supone un grave peligro para la

integridad de los datos

- Dependiendo de las acciones del atacante, podría bloquear el acceso a los sistemas o interrumpir servicios. Así que supone un grave peligro

ORIGEN DEL INCIDENTE

- El origen del incidente puede ser tanto externo como interno. Externo debido a que el atacante explota una vulnerabilidad que ha sido investigada y buscada por este para ejecutar código. Pero también interna ya que la empresa no tuvo en cuenta dicha vulnerabilidad y gracias a eso el atacante puedo explotarla.

NIVEL DE CRITICIDAD

- El nivel de criticidad es bastante alto. El atacante al haber explotado esa vulnerabilidad puede hacer prácticamente lo que quiera ejecutando código malicioso. Esto repercute bastante en la seguridad de la información y la operativa de la empresa.

ATAQUE 9:

Un hospital es víctima de un ataque que cifra todos sus sistemas críticos, incluyendo las bases de datos de pacientes. Los atacantes exigen un pago en bitcoins a cambio de la clave de descifrado. La operación del hospital queda paralizada hasta que se resuelve el incidente.

TIPO DE INCIDENTE

- Este se trata de un Ransomware
- Un Ransomware es un malware que lo que hace es impedir el uso de los equipos que se tiene ya sea a particulares o a toda una empresa. Cifrando así también los archivos e incluso pidiendo un monto de dinero. Es lo que ha ocurrido en este caso.

MODELO CIA

- En cuanto a la confidencialidad de la información, si se ve afectada ya que la información de los pacientes está totalmente cifrada. Además de hablamos de un hospital por lo cual el riesgo es mayor
- En cuanto a la integridad, los datos se ven comprometidos ya que el Ransomware se dedica a bloquear absolutamente todo por lo cual al no poderse utilizar equipos, tampoco se puede modificar la información por parte del hospital
- La disponibilidad es una de las cosas mas importantes que necesita un hospital y este ataque provoca un problema extremadamente grave al no poder utilizar los equipos informáticos para ayudar a los pacientes. La disponibilidad se ve completamente comprometida

ORIGEN DEL INCIDENTE

- El ataque en este caso es externo ya que los atacantes utilizan herramientas para cifrar los sistemas del hospital. No obstante es importante no descartar que algún ordenador fuese infectado anteriormente y los atacantes hayan aprovechado eso para entrar y obtener acceso a todos los ordenadores, infectarlos y realizar el ataque.

NIVEL DE CRITICIDAD

- Este ataque es demasiado peligroso sobre todo en el ámbito que se esta realizando es decir un hospital. Que todos los equipos estén cifrados hace que el movimiento que hay en el hospital se paralice hasta que puedan descifrarlos

ATAQUE 10:

Una empresa deja accesible al público su servidor de almacenamiento en la nube sin aplicar restricciones adecuadas de acceso. Un atacante descubre esto y accede a la información sensible almacenada en el servidor, incluyendo documentos internos y datos financieros.

TIPO DE INCIDENTE

- Se trata de una exposición de datos
- Exponer datos sin seguridad a la red es bastante peligroso especialmente si somos una empresa que maneja bastante esos datos. En este caso un atacante ha descubierto esto y se ha aprovechado.

MODELO CIA

- La confidencialidad de la información esta en peligro ya que la propia empresa ha dejado al descubierto todo. De tal manera que el atacante se aprovechó
- La integridad de la información dependerá del atacante. Si el atacante modifica o elimina datos, la integridad de la información se verá comprometida. De lo contrario la información estará a salvo dependiendo de las herramientas que utilice la empresa para poder cifrarla.
- La disponibilidad de los servicios no necesariamente debe de estar comprometida. Ya que el ataque se dedica a el robo de los datos.

ORIGEN DEL INCIDENTE

- El origen del incidente ha sido principalmente interno debido que ha sido problema de la empresa dejar expuesta la información importante. El problema ha sido también cuando el atacante ha sabido donde buscar y ha encontrado esa información que no estaba protegida.

NIVEL DE CRITICIDAD

- El nivel de criticidad ha sido bastante alto debido a la exposición de información sensible y el posible impacto en la reputación y las finanzas de la empresa.