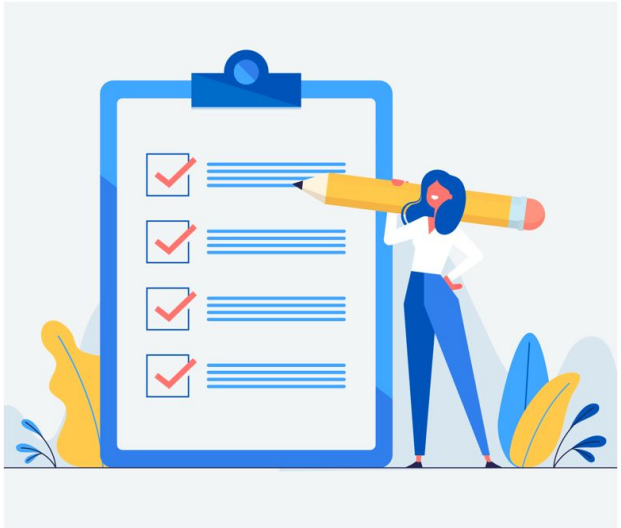
Actividad Tipos de Amenazas

Utilizando este documento de presentación, cada mesa deberá resolver y completar en cada hoja , que le corresponde según su número de mesa.



Mesa 1

Nota :

<https://docs.google.com/document/d/1yk1W6jFx5LWfRcFQCWkraPs96ZF-2DGoSaFnpIAS0n8/edit>

¿Qué tipo de amenaza es?

¿Cómo comienza y cómo se propaga esta amenaza?

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?

Mesa 2

Nota:
<https://www.welivesecurity.com/la-es/2021/06/10/backdoordiplomacy-actualizando-quarian-turian-backdoor-utilizado-contra-organizaciones-diplomaticas/
¿Qué tipo de amenaza es? troyano backdoor
¿Cómo comienza y cómo se propaga esta amenaza? consiste en explotar aplicaciones vulnerables expuestas a Internet en servidores web.
¿Hay más de una amenaza aplicada ?
¿Qué solución o medida recomendarían ? Correr el antivirus y como medida de prevención mantener copias de seguridad actualizadas.

Mesa 3

Nota : https://www.welivesecurity.com/la-es/2021/04/08/vyveva-nuevo-backdoor-grupo-apt-lazarus/

¿Qué tipo de amenaza es? Backdoor y spyware

¿Cómo comienza y cómo se propaga esta amenaza?

Comienza con el backdoor que descarga el spyware en la computadora (instalador) y no se propaga, es dirigido.

¿Hay más de una amenaza aplicada? Si, el backdoor y el spyware.

¿Qué solución o medida recomendarían? Con un antivirus y antispyware y escanear todas las computadoras de la red. Tener copias de seguridad para restaurar en caso necesario de pérdida de información.

Mesa 4

Nota : https://www.welivesecurity.com/la-es/2021/02/02/kobalos-amenaza-linux-afecta-infraestructuras-informaticas-alto-rendimiento/

¿Qué tipo de amenaza es? Malware/**troyano** que crea backdoors para robar credenciales utilizando un cliente OpenSSH “troyanizado” (supercomputadores (HPC) y servidores que operan con Linux, FreeBSD y Solaris, aunque no se descarta que haya variantes para Windows)

¿Cómo comienza y cómo se propaga esta amenaza? No pudo determinarse, se pudo investigar que una de las causantes haya sido utilizar SO no actualizados, sin soporte o parches. Esto generó mayor vulnerabilidad

Kobalos otorga acceso remoto al sistema de archivos, brinda la capacidad de generar sesiones de terminal y permite conexiones de proxy a otros servidores infectados por Kobalos

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ? La configuración de la autenticación de dos factores para conectarse a servidores SSH mitigará la amenaza, ya que el uso de credenciales robadas parece ser una de las formas en que se puede propagar a diferentes sistemas.

Mesa 5

Nota : <Poner el link>

¿Qué tipo de amenaza es?

¿Cómo comienza y cómo se propaga esta amenaza?

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?

Mesa 6

Nota : link

¿Qué tipo de amenaza es? Troyano

¿Cómo comienza y cómo se propaga esta amenaza?

Por descarga y winrar auto ejecutable. Utiliza correos electrónicos maliciosos como mecanismo de distribución

¿Hay más de una amenaza aplicada ? Si, dos

¿Qué solución o medida recomendarían ? no vivan en [Croacia, Serbia, Montenegro, Bosnia y Herzegovina] y fijense que mail abren y revisar los archivos adjuntos

Mesa 7

Nota : <**https://www.welivesecurity.com/la-es/2021/07/05/ataque-masivo-ransomware-revil-comprometio-mas-1000-companias-mundo/**>

¿Qué tipo de amenaza es? **Ransomware**

¿Cómo comienza y cómo se propaga esta amenaza? Comienza mediante la actualización automática del software de gestiónTI Kaseya VSA y se propaga mediante la actualización con permisos de administrador donde afectó a los MSP y estos a su vez infectaron los sistemas de los clientes

¿Hay más de una amenaza aplicada ? no

¿Qué solución o medida recomendarían? No pagar. Y mantener los backups actualizados

Mesa 8

Nota: LINK

¿Qué tipo de amenaza es? Ransomware Darkside

¿Cómo comienza y cómo se propaga esta amenaza? Se estima que fue a través del protocolo RDP (Es el protocolo que se utiliza para hacer trabajo remoto). Se cree que se propagó a través de los escritorio remotos, vulnerando la red a través de ataques a las credenciales del RDP.

¿Hay más de una amenaza aplicada ? No, sólo fue el ransomware

¿Qué solución o medida recomendarían ?

No pagar el rescate (por recomendación del FBI)
No tener información en un mismo lugar, tener backups actualizados.
Descargar un producto de seguridad conocido para la desinfección
Capacitar a los empleados para evitar futuros cyberataques.

Mesa 9

Nota : <Poner el link>

¿Qué tipo de amenaza es?

¿Cómo comienza y cómo se propaga esta amenaza?

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?

Mesa 10

Nota :

¿Qué tipo de amenaza es?

¿Cómo comienza y cómo se propaga esta amenaza?

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?

Mesa 12

Nota : <Poner el link>

¿Qué tipo de amenaza es?

¿Cómo comienza y cómo se propaga esta amenaza?

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?