LABORATORIO 3: El Incidente Crítico

JULIANA TORRES AARÓN

Objetivos del Laboratorio:

1. **Identificar el vector de ataque inicial (e.g., phishing, explotación de vulnerabilidad).**

- Si el phishing es identificado: Que se debe buscar.

Cuando se identifica que el vector de ataque inicial puede ser un caso de phishing, es fundamental realizar una revisión detallada de ciertos elementos clave para confirmar la amenaza. Primero se debe buscar correos electrónicos sospechosos que presenten remitentes falsificados o dominios similares a los oficiales (por ejemplo, direcciones como @empresax-support.com que imitan al dominio legítimo @empresax.com). También es importante identificar asuntos con tono urgente o alarmista, tales como “¡Tu cuenta será suspendida!” o “Acción requerida inmediatamente”, ya que buscan generar presión sobre el usuario para que actúe sin pensar.

Otro indicador relevante es la presencia de archivos adjuntos que puedan contener macros o scripts maliciosos, así como enlaces dentro del correo que redirijan a páginas falsas que imitan el sitio web oficial de la empresa, con el objetivo de engañar al usuario y obtener credenciales o información sensible. Además, se deben tener en cuenta las solicitudes directas de información confidencial, como contraseñas o datos bancarios, ya que son una señal clara de intento de fraude.

Por último, es esencial identificar si algún usuario ha hecho clic en enlaces o descargado archivos sospechosos y ha reportado comportamientos anómalos en sus equipos, como lentitud, aparición de procesos extraños o bloqueo de funciones, lo cual puede ser una señal de que el ataque ha tenido éxito.

2. **Analizar los logs del sistema para encontrar evidencias de actividad maliciosa.**
   Una vez identificado el posible ataque de phishing, se debe realizar un análisis detallado de los logs del sistema, de correo electrónico, firewall y autenticación. En estos registros es posible encontrar evidencia como:
   Intentos de inicio de sesión fallidos o inusuales, especialmente desde ubicaciones geográficas atípicas.
   Accesos a enlaces sospechosos incluidos en los correos, reflejados en los logs de navegación o DNS.
   Descarga de archivos ejecutables desde dominios no confiables.
   Ejecución de procesos inusuales iniciados poco después de la interacción con el correo malicioso.

Modificaciones en permisos o creación de cuentas no autorizadas en el sistema.
Estos datos permiten confirmar si el phishing fue exitoso y si algún equipo comenzó a actuar de forma anómala.

3. **Determinar el alcance del compromiso y los sistemas afectados.**
   Con base en la evidencia obtenida, es necesario determinar cuántos usuarios interactuaron con el correo malicioso, qué tipo de archivos descargaron o ejecutaron, y si ingresaron información confidencial.
   También se debe verificar si:
   Se ha producido una filtración de credenciales.
   Algún equipo ha sido infectado con malware o está actuando como punto de entrada para nuevos ataques.
   Se han detectado comunicaciones con servidores externos desconocidos (posible exfiltración de datos).
   Otros sistemas conectados en la red interna presentan signos similares de compromiso.

4. **Proponer medidas de contención y recuperación**
   Para contener el ataque y evitar su propagación, es crucial aislar de inmediato los equipos comprometidos, eliminar los correos maliciosos mediante filtrado, actualizar las herramientas de seguridad y forzar el cambio de todas las credenciales. Además, se deben revisar las configuraciones de los sistemas y activar medidas como la autenticación multifactor (MFA). En la fase de recuperación, es fundamental restaurar los sistemas desde copias de seguridad limpias, documentar el incidente y capacitar al personal para detectar y reportar futuros intentos de phishing**.**