Laboratorio 3

Estudiante: Hernan Andres Gutierrez Anillo

Paso 1:Identificar el Vector de Ataque Inicial

1.1 Revisión de Indicadores Iniciales
Al identificar un posible incidente de phishing, es esencial recopilar la siguiente información para detectar los primeros signos:

-Mensajes Extraños: Un usuario informa que recibió un correo electrónico de una fuente desconocida con un enlace o archivo adjunto.

-Fallos en Sistemas Específicos: Los usuarios empiezan a reportar fallos en sistemas o aplicaciones, tal vez relacionados con un acceso no autorizado o la ejecución de un código malicioso.

Posibles Indicadores de Phishing:
-Correos electrónicos sospechosos con asuntos que llaman la atención (por ejemplo, "Urgente: Actualización de Seguridad de tu Cuenta").

-Archivos adjuntos maliciosos (como archivos .exe, .zip, .docm) que intentan instalar malware o un troyano.

-Enlaces fraudulentos que intentan redirigir a los usuarios a sitios web de phishing que se hacen pasar por sitios legítimos (como un banco o plataforma de correo).

1.2 Evaluación de la Evidencia
En caso de identificar phishing, deberíamos buscar lo siguiente:

Revisar el encabezado del correo: Validar si la dirección de correo electrónico del remitente es legítima. Muchas veces, los correos de phishing tienen direcciones ligeramente alteradas o fraudulentas.

Analizar los archivos adjuntos: Si el correo contiene archivos, revisar los metadatos y los posibles indicadores de malware.

Revisar los enlaces del correo: Verificar que los enlaces en el correo coincidan con la URL legítima (por ejemplo, la URL de un banco legítimo).

Paso 2: Analizar los Logs del Sistema
2.1 Recolección de Logs
Para identificar la actividad maliciosa relacionada con el ataque de phishing, revisamos los logs de los siguientes sistemas:

Servidor de Correo Electrónico:
Buscar los correos electrónicos recibidos, especialmente los que contienen archivos adjuntos sospechosos o enlaces a sitios desconocidos. Se puede revisar si hay múltiples intentos de acceso fallidos, lo cual puede indicar un intento de phishing.

Sistema de Bases de Datos:
Verificar si ha habido accesos no autorizados a bases de datos relacionadas con los usuarios objetivo del phishing. Puede haber intentos de extracción de datos sensibles.

Logs de Seguridad del Sistema:
Revisar los logs de firewall y antivirus para detectar alertas de accesos sospechosos o archivos maliciosos que fueron bloqueados.

2.2 Análisis de la Actividad Maliciosa
Se debe realizar un análisis para identificar patrones inusuales que sugieran que el incidente fue causado por un ataque de phishing:

-Revisar accesos inusuales: Si un usuario abrió un archivo adjunto malicioso, revisar si hay conexiones inusuales desde su cuenta a otros sistemas críticos.

-Revisar los logs de correos electrónicos: Verificar si el mensaje de phishing fue enviado a múltiples usuarios o si hubo reenvíos a otras cuentas externas.

Herramientas de Análisis:

Wireshark: Para analizar tráfico de red y detectar comunicaciones sospechosas.

Splunk o ELK Stack: Para realizar búsquedas avanzadas y crear alertas en los logs.

Sysinternals: Para examinar comportamientos anómalos del sistema en estaciones de trabajo afectadas.

Paso 3: Determinar el Alcance del Compromiso
3.1 Identificación de Sistemas Comprometidos
Una vez identificado que el ataque fue mediante phishing, debemos:

-Revisar sistemas afectados: Identificar qué estaciones de trabajo, servidores o cuentas de usuario han sido comprometidos.

-Verificar si hay propagación lateral: Comprobar si el malware en los sistemas afectados intentó propagarse a otras máquinas de la red.

Evaluación:
Si un usuario de correo electrónico fue comprometido, verificar si otros usuarios también recibieron correos de phishing del mismo remitente.

3.2 Evaluación del Impacto
Evaluar los posibles daños causados por el ataque:

Disponibilidad: ¿Hubo alguna interrupción del servicio debido al ataque? ¿Los sistemas estuvieron fuera de línea por algún periodo?

Integridad: ¿El ataque afectó la integridad de los datos o sistemas? (por ejemplo, cambios no autorizados en datos o configuraciones).

Confidencialidad: ¿Hubo filtración de información sensible como credenciales de usuario o datos financieros?

Resultado Esperado:
Definir la gravedad del incidente en términos de impacto en la disponibilidad, integridad y confidencialidad de los datos.

Paso 4: Proponer Medidas de Contención y Recuperación
4.1 Medidas de Contención Inmediatas
Tomar medidas inmediatas para evitar que el ataque de phishing se propague:

-Desconectar sistemas comprometidos de la red: Aislar las estaciones de trabajo o servidores infectados para evitar la propagación del malware.

-Cambiar credenciales de acceso: Pedir a los usuarios afectados que cambien sus contraseñas, especialmente si se comprometieron sus credenciales por el phishing.

-Aplicar parches y actualizaciones: Si el phishing se utilizó para explotar alguna vulnerabilidad, asegurarse de que todos los sistemas estén actualizados.

4.2 Plan de Recuperación
Una vez contención, es crucial restaurar los sistemas comprometidos:

Restaurar sistemas desde copias de seguridad confiables.

Verificar la integridad de los sistemas después de la restauración y comprobar que no haya restos de malware.

Monitorear el sistema: Durante el proceso de recuperación, asegurar que no haya nuevas alertas o accesos no autorizados.

4.3 Comunicación Post-Incidente
Una vez resuelto el incidente, es fundamental informar a todas las partes interesadas:

Notificar al equipo de TI y a los usuarios afectados sobre el ataque, las medidas tomadas y los pasos a seguir.

Informar a la dirección de la empresa sobre el impacto del incidente y las medidas implementadas para prevenir futuros ataques.