Laboratorio3

Escenario:

Un empleado abrió un correo de cambio de contraseña de la empresa, dando sus datos a esta página supuestamente legitima, dando datos importantes en el camino.

Paso 1: **Identificar el Vector de Ataque Inicial**

En este caso, el vector de ataque inicial fue **phishing por correo electrónico**.

Un atacante envió un correo electrónico que **simulaba ser legítimo**, probablemente haciéndose pasar por el departamento de TI o un sistema automático de la empresa, solicitando un **cambio de contraseña**. Este correo contenía un enlace a una página web fraudulenta que imitaba una página oficial.

Paso 2: Analizar los Logs del Sistema para Encontrar Evidencias de Actividad Maliciosa

Logs del Servidor de Correo Electrónico:

Los servidores de correo electrónico son un punto clave en un ataque de phishing, ya que se origina desde allí el envío del correo malicioso. Los logs que se deben revisar incluyen:

- **Registros de entrega de correos (logs de SMTP)**: Para identificar si el correo malicioso fue enviado desde una fuente externa o comprometida.
    - Buscar la dirección IP de origen y verificar si corresponde a una IP legítima o si está asociada a actividades maliciosas.
    - Revisa los encabezados de los correos electrónicos para determinar si la dirección "De" o "Reply-To" está suplantada.
    - Revisa si el correo ha sido marcado como spam, si hubo intentos fallidos de entrega o rebotados.
- **Logs de autenticación y acceso**:
    - Determina si alguien ha iniciado sesión en el sistema de correo con credenciales sospechosas o no autorizadas.

    - Identifica los usuarios que han accedido desde ubicaciones geográficas inusuales o dispositivos desconocidos.

- **Logs de envío de correos**: Para revisar si algún usuario ha enviado correos masivos o correos con enlaces sospechosos.

Logs del Sistema de Bases de Datos:

En los sistemas de bases de datos, es crucial verificar cualquier acceso o modificación a datos sensibles, especialmente si el atacante tuvo acceso a credenciales. Los logs importantes son:

- **Registros de acceso**: Identificar accesos no autorizados a la base de datos o conexiones inusuales (por ejemplo, fuera del horario laboral o desde una IP extraña).
    - Busca patrones de consultas que extraigan datos sensibles (como contraseñas, información personal o transacciones).
- **Logs de autenticación**: Determinar si las credenciales de los usuarios afectados fueron usadas para acceder a la base de datos.
- **Registros de modificaciones**: Revisa las tablas que han sido modificadas, insertadas o eliminadas, para identificar si algún dato relevante ha sido alterado de forma inusual.

Logs de Seguridad:

Aquí se debe revisar cualquier tipo de alerta que haya sido generada por sistemas de seguridad, como firewall, antivirus, IDS (Sistema de detección de intrusiones), entre otros.

- **Alertas de seguridad**: Busca alertas de acceso no autorizado, intentos de explotación de vulnerabilidades, cambios en las configuraciones de seguridad o en las políticas de firewall.
- **Logs de tráfico de red**: Identificar tráfico saliente hacia direcciones IP sospechosas o inusuales que puedan estar relacionadas con el servidor de phishing o que indiquen exfiltración de datos.
- **Registros de antivirus o EDR**: Verifica si se detectaron malware o actividades sospechosas en los endpoints de los usuarios afectados.

2.2 Análisis de la Actividad Maliciosa

Análisis de los Logs para Buscar Patrones Inusuales:

- **Patrones en los correos electrónicos**: Si se revisan varios correos de phishing, se pueden identificar patrones recurrentes como ciertos dominios de envío, direcciones de IP, frases comunes o formatos de correo.

    - Comparar el formato, remitente y asunto de los correos para ver si hay coincidencias con otros intentos de phishing.
    - Revisa si las URLs contenían redirecciones a sitios web maliciosos o de suplantación.
- **Accesos inusuales**: Revisa si los usuarios afectados accedieron a sistemas o servicios en momentos o desde ubicaciones inusuales.
    - Analiza los logs de acceso a sistemas, buscando inicios de sesión fuera del horario laboral, desde dispositivos no autorizados, o desde nuevas ubicaciones geográficas.
    - Busca en los logs si el atacante ha intentado o logrado elevar privilegios en el sistema.
- **Consultas inusuales en bases de datos**: Compara las consultas realizadas contra las que normalmente se ejecutan en el sistema. Las consultas masivas o de extracción de datos pueden ser una señal de que los atacantes están buscando información sensible.
- **Conexiones maliciosas o no autorizadas**: Si se encuentran conexiones a servidores externos, especialmente hacia direcciones IP que no deberían estar involucradas con las operaciones normales, podría indicar la exfiltración de datos o comunicación con un servidor de comando y control (C&C).

Herramientas de Análisis para los Logs:

Existen diversas herramientas que pueden ayudar en el análisis de logs:

- **SIEM (Security Information and Event Management)**: Herramientas como **Splunk**, **LogRhythm** o **Elastic Stack (ELK)** permiten centralizar y analizar grandes volúmenes de logs, facilitando la detección de patrones maliciosos y correlacionando eventos de diferentes sistemas.
- **Kali Linux y herramientas de análisis forense**: Herramientas como **Wireshark** (para analizar tráfico de red), **Volatility** (para análisis forense de memoria) y **OSSEC** (para monitoreo de seguridad y detección de intrusos) son útiles para detectar actividad anómala.
- **Syslog y herramientas de monitoreo de red**: Herramientas como **Zeek** (anteriormente conocido como Bro) o **Suricata** ayudan a monitorizar el tráfico de red y detectar actividades sospechosas o patrones de comportamiento no usuales.
- **Antivirus/EDR (Endpoint Detection and Response)**: Plataformas como **CrowdStrike**, **Carbon Black** o **Symantec EDR** permiten detectar y analizar comportamientos maliciosos en los endpoints.

- **Herramientas específicas de bases de datos**: Para el análisis de logs de bases de datos, herramientas como **Oracle Audit Vault**, **SQL Server Profiler** y **MySQL Enterprise Audit** son esenciales para revisar accesos y actividades inusuales en bases de datos.

Paso 3: Determinar el Alcance del Compromiso y los Sistemas Afectados

3.1 Identificación de Sistemas Comprometidos:

Una vez que se ha identificado que un empleado ha caído en un ataque de phishing, el siguiente paso es identificar los sistemas comprometidos y determinar el alcance del ataque. Aquí se deben realizar las siguientes actividades:

Revisar los sistemas interconectados:

- **Redes y Conexiones**: Se debe revisar la infraestructura de red para identificar posibles movimientos laterales del atacante. Esto incluye servidores, estaciones de trabajo y otros dispositivos conectados a la red que puedan haberse visto comprometidos como resultado de credenciales comprometidas.
    - **Revisión de conexiones de red**: Monitorear conexiones sospechosas entre dispositivos comprometidos y otros sistemas internos o externos. El análisis de tráfico de red y la correlación de logs de firewall y switches puede ayudar a detectar actividad anómala.
    - **Revisión de permisos compartidos**: Verificar si los atacantes aprovecharon las credenciales comprometidas para escalar privilegios en sistemas interconectados.
- **Revisión de acceso a sistemas críticos**: Identificar si los atacantes han tenido acceso a sistemas esenciales como servidores de bases de datos, sistemas financieros, plataformas de comunicación interna, etc.
    - Si los atacantes han obtenido acceso a sistemas críticos, se deben aislar inmediatamente esos sistemas y revocar accesos no autorizados.

Evaluar el impacto en la infraestructura crítica:

- **Infraestructura de TI**: Determina si los sistemas comprometidos incluyen infraestructura crítica como servidores de correo, sistemas de base de datos, servicios en la nube, aplicaciones empresariales clave o recursos de infraestructura de red.
    - **Control de acceso y gestión de identidades**: Analizar si el atacante ha obtenido acceso a cuentas privilegiadas o si se han creado nuevas cuentas maliciosas con privilegios elevados.

    - **Sistemas de respaldo**: Revisar los sistemas de respaldo para verificar si los datos han sido modificados o si los atacantes han intentado cifrar o eliminar copias de seguridad.

3.2 Evaluación del Impacto:

Evaluar el impacto del compromiso es crucial para determinar el daño y la respuesta adecuada. En este paso se deben considerar tres aspectos clave: **disponibilidad**, **integridad** y **confidencialidad** de los datos.

Disponibilidad:

- **Interrupción de servicios**: Determinar si el atacante ha causado interrupciones en los servicios críticos, como la imposibilidad de acceder a servidores, bases de datos o aplicaciones debido a ataques como denegación de servicio (DoS) o cambios en la configuración de los sistemas.
    - ¿Los usuarios experimentaron caídas de servicio o tiempos de inactividad?
    - **Acceso a datos**: Evaluar si los usuarios o sistemas legítimos pueden seguir accediendo a los datos o si las herramientas de trabajo de la empresa han sido afectadas.
- **Impacto en la continuidad del negocio**: Determinar si el incidente ha afectado la capacidad de la empresa para operar de manera efectiva. Si se interrumpieron procesos de negocio críticos, esto debería ser priorizado en la evaluación.

Integridad:

- **Modificación no autorizada de datos**: Evaluar si los atacantes han tenido acceso a datos sensibles y si esos datos fueron modificados, alterados o eliminados. Esto puede incluir la alteración de registros financieros, contratos o cualquier información clave.
    - ¿El atacante cambió las contraseñas o las configuraciones de los sistemas?
    - ¿Hubo un intento de manipulación de datos o registros?
- **Registro de actividades**: Verificar si los logs del sistema fueron manipulados para ocultar las acciones del atacante. La integridad de los registros de auditoría debe ser cuidadosamente evaluada, ya que esto puede ser indicativo de un intento de encubrimiento por parte del atacante.

Confidencialidad:

- **Exfiltración de datos**: Determinar si el atacante ha tenido acceso a datos confidenciales, como información personal identificable (PII), datos financieros, registros de clientes, etc. Además, identificar si estos datos han sido extraídos de forma no autorizada.
    - ¿Se ha detectado tráfico hacia servidores externos o direcciones IP que sugieren la exfiltración de datos?
    - ¿El atacante descargó archivos sensibles o accedió a bases de datos críticas?
- **Acceso a información confidencial**: Asegurarse de que los sistemas comprometidos no contengan acceso a información sensible que pueda ser utilizada para futuros ataques o para daño reputacional.

Resultado Esperado:

Una vez completada la evaluación, el resultado esperado es tener una comprensión clara de los siguientes puntos:

1. **Sistemas afectados**: Conocer qué sistemas específicos (servidores, estaciones de trabajo, bases de datos) han sido comprometidos.
2. **Alcance del ataque**: Cuántos usuarios, datos y sistemas se han visto afectados, y si los atacantes han tenido acceso a sistemas críticos o datos sensibles.
3. **Impacto en la empresa**: Cuánto ha afectado el incidente a la disponibilidad de los servicios, la integridad de los datos y la confidencialidad de la información sensible.
4. **Acción inmediata**: Identificar los pasos inmediatos para contener el ataque y prevenir mayores daños, como el aislamiento de los sistemas comprometidos, la revocación de accesos y la notificación a las autoridades pertinentes si es necesario.

Paso 4: Proponer Medidas de Contención Inmediatas

4.1 Medidas de Contención Inmediatas

Una vez que se ha identificado el ataque, se deben implementar medidas inmediatas para detener el ataque, limitar su propagación y proteger los sistemas restantes. Las medidas clave son:

Desconectar sistemas comprometidos:

- **Aislamiento de los sistemas afectados**: Los sistemas comprometidos deben ser desconectados inmediatamente de la red para evitar la

propagación del ataque. Esto incluye estaciones de trabajo, servidores, bases de datos o cualquier dispositivo que haya mostrado señales de compromiso.

    - Asegurarse de que los sistemas de correo electrónico y las aplicaciones críticas no estén en contacto con la red para impedir que el atacante continúe su actividad maliciosa o exfiltre datos.
    - Deshabilitar el acceso remoto a los sistemas afectados y cerrar las conexiones de red sospechosas.

Actualización de sistemas:

- **Parches y actualizaciones**: Si el atacante ha explotado alguna vulnerabilidad en el sistema, es crucial aplicar los parches de seguridad y actualizaciones que puedan haber sido ignorados previamente.
    - Revisa las versiones de software y asegúrate de que todos los sistemas estén actualizados con los últimos parches de seguridad.
    - Verificar si el sistema operativo, las aplicaciones y los servicios clave tienen vulnerabilidades conocidas que deban ser abordadas inmediatamente.
- **Revisión de configuraciones de seguridad**: Asegúrate de que las configuraciones de seguridad estén actualizadas para minimizar las oportunidades de que un atacante pueda explotar otras debilidades en el sistema.

Cambio de credenciales:

- **Revocar y cambiar contraseñas**: Los usuarios afectados y aquellos con acceso a sistemas críticos deben cambiar inmediatamente sus contraseñas.
    - Asegúrate de que las contraseñas sean fuertes y únicas, y que no se repitan entre distintos sistemas.
    - Hacer uso de autenticación multifactor (MFA) para los accesos a sistemas importantes, si no estaba habilitada previamente.
    - Revocar credenciales de usuarios que no estén autorizados o que hayan sido comprometidas.

4.2 Plan de Recuperación

El objetivo de la recuperación es restaurar los sistemas comprometidos a su funcionamiento normal y minimizar el impacto en el negocio.

Restauración desde Copias de Seguridad:

- **Verificar la integridad de las copias de seguridad**: Antes de restaurar los sistemas desde copias de seguridad, asegúrate de que las copias no estén comprometidas y sean válidas.
    - Si los sistemas afectados tienen copias de seguridad actualizadas, se deben restaurar para devolver los sistemas a su estado anterior al ataque.
    - Si hay sospecha de que las copias de seguridad también pueden estar comprometidas, se debe realizar un análisis exhaustivo de su integridad.
- **Restauración progresiva**: Restaurar los sistemas en fases, comenzando con los sistemas menos críticos y asegurando que la infraestructura principal (como servidores de bases de datos o aplicaciones esenciales) se recupere correctamente.

Monitoreo y Validación:

- **Monitoreo post-restauración**: Una vez restaurados los sistemas, es crucial monitorear su actividad para detectar cualquier señal de que el atacante aún tenga acceso o haya dejado alguna puerta trasera.
    - Utilizar herramientas de monitoreo en tiempo real (como SIEM o sistemas de detección de intrusiones) para observar el tráfico y las actividades de los usuarios.
    - Asegúrate de que todas las conexiones sean legítimas y que no haya anomalías en los registros de acceso.
- **Validación de seguridad**: Validar que los sistemas restaurados estén completamente seguros. Esto puede incluir realizar auditorías de seguridad, pruebas de penetración o análisis forense para asegurarse de que no queden vulnerabilidades abiertas.

Evaluación Post-Incidente:

- **Análisis de causa raíz**: Investigar cómo ocurrió el ataque, qué vulnerabilidad se explotó y si los controles de seguridad existentes fueron suficientes para prevenirlo.
    - Realizar un informe detallado sobre cómo se propagó el ataque y qué aspectos de la infraestructura o políticas de seguridad fallaron.
- **Revisión de las lecciones aprendidas**: Evaluar el desempeño del equipo durante el incidente y las medidas de respuesta. Analizar lo que funcionó bien y lo que necesita ser mejorado para futuros incidentes.

4.3 Comunicación

La comunicación es esencial durante un incidente de seguridad. Es importante que todas las partes interesadas sean informadas adecuadamente para tomar las decisiones correctas y gestionar la respuesta.

¿A quién se le debe informar?

- **Equipo de respuesta a incidentes (IRT)**: Asegúrate de que todos los miembros clave del equipo de respuesta, incluidos los responsables de IT, seguridad, comunicaciones, legal y gestión, estén informados de la situación y el progreso de las acciones.
- **Dirección de la empresa**: La alta dirección debe ser informada sobre el impacto, las medidas que se están tomando y los próximos pasos. Esto es especialmente importante si el ataque ha afectado a información confidencial o ha tenido impacto en los clientes.
- **Empleados afectados**: Los empleados cuyo trabajo o sistemas fueron comprometidos deben ser informados sobre las medidas que deben tomar (como el cambio de contraseñas) y sobre las políticas de seguridad que deben seguir durante y después del incidente.
- **Clientes y terceros**: Si la seguridad de los datos de los clientes se ha visto comprometida o el servicio ha sido afectado, se debe notificar a los clientes y socios comerciales. Esto debe hacerse de manera transparente y siguiendo los procedimientos legales y regulatorios de notificación de brechas de seguridad.

Transparencia:

- **Claridad en la comunicación**: La información proporcionada debe ser clara, precisa y coherente. Evitar el pánico y proporcionar detalles específicos sobre lo que se está haciendo para mitigar los daños.
    - Explicar las medidas que se están tomando para contener el ataque y restaurar los sistemas, así como cualquier cambio que los usuarios deban implementar en sus sistemas o cuentas.
- **Documentación y seguimiento**: Mantener un registro detallado de todas las comunicaciones realizadas, tanto internas como externas, para asegurar que no haya confusión y para cumplir con los requisitos legales.