Laboratorio 3 Roberts Pertuz

Paso 1: Identificar el Vector de ataque inicial

- Correos electrónicos sospechosos
- Se reportan mensajes y bloqueos inusuales
- Fallos en servicios importantes(correos, clavee, datos)
- Alertas de antivirus

Posibles Vectores:

- Phishing: Mensajes engañosos que buscan credenciales.
- Explotación de vulnerabilidad: Servicios desactualizados con fallos conocidos.
- Acceso no autorizado: Usuarios que inician sesión desde ubicaciones inusuales.

1.2 Evaluación de la Evidencia

- **Si el phishing es identificado:**
  Buscar encabezados de correos, enlaces maliciosos, archivos adjuntos sospechosos y direcciones IP de origen.
- **Si hay sospecha de vulnerabilidad:**
  Revisar versiones de software, servicios públicos expuestos (puertos abiertos) y logs de escaneo previos al ataque.

Resultado esperado:
Determinar que el ataque comenzó con un **correo phishing con un archivo adjunto malicioso (ej: factura.docm con macro)**.

Paso 2: Analizar l s Logs del Sistema para encontrar Evidencias de Actividad Maliciosa

2.1 Recolección de Logs

Logs a revisar:

- **Correo electrónico:**
  - Buscar correos enviados desde dominios sospechosos.
  - Revisar quién abrió o descargó el archivo.
  - Revisar el cuerpo del correo
- **Bases de datos:**
  - Consultas extrañas, especialmente fuera del horario laboral.
  - Accesos no autorizados o desde IPs externas.
  - Injeccion de dependencias
- **Seguridad (firewall, antivirus):**
  - Alertas de malware.
  - Cambios en las políticas de seguridad.
  - Fallos de autenticación o accesos desde direcciones desconocidas.

2.2 Análisis de Actividad Maliciosa

- Buscar picos de actividad inusual (muchas conexiones, tráfico fuera de horario).
- Comparar contra comportamientos normales de los usuarios.
- Verificar si hubo intentos de escalamiento de privilegios.

Herramientas sugeridas:

- Antivirus, visor de sucesos, seguridad del las apps de correo(Gmail, Outlook, Hotmail), observación y algunas alertas notorias que se puedan apreciar

Paso 3: Determinar el Alcance del Compromiso y los sistemas afectados

3.1 Identificación de Sistemas Comprometidos

Acciones:

- Listar los equipos que interactuaron con el adjunto malicioso.
- Verificar si hay comunicación con servidores externos (exfiltración).
- Revisar si el malware se replicó por red.
- Realizar análisis de los daños afectados al equipo
- Verificar la base de datos

Evaluación del impacto en infraestructura crítica:

- ¿El ataque alcanzó servidores, backups, sistemas de autenticación?
- ¿Qué daños causó?
- Verificar cuentas privilegiadas

3.2 Evaluación del Impacto

Criterios:

- **Disponibilidad:**
  ¿Los sistemas están funcionando correctamente?
- **Integridad:**
  ¿Los datos fueron modificados o borrados?
- **Confidencialidad:**
  ¿Se filtraron datos sensibles (clientes, contraseñas, etc.)?

Paso 4: Medidas de Contención y Recuperación

4.1 Contención Inmediata

Acciones rápidas:

- **Desconectar** los sistemas comprometidos de la red.
- **Actualizar** el software vulnerable.
- **Cambiar credenciales** comprometidas de inmediato.

4.2 Plan de Recuperación

- **Restaurar desde backups seguros.**
- **Monitorear** los sistemas restaurados para detectar reinfecciones.
- **Validar** la integridad de los datos restaurados.

- **Evaluación post-incidente:** Documentar el incidente, mejorar controles y capacitar al personal.

4.3 Comunicación

Se debe informar a:

- Personal de TI y seguridad.
- Gerencia.
- Usuarios afectados (si aplica).
- Posiblemente entidades externas (proveedor de correo, CERT nacional).

Transparencia:
Mantener un canal abierto sobre las acciones tomadas y los riesgos mitigados.