Roberto Blanco

Laboratorio #3 Ciberseguridad

Paso #1

¿Qué ataque recibiste?

R/ Virus Gusano

¿Por qué?

R/ Me conecté a una red de una biblioteca y esa red tenia o contaba con uno de estos virus, como no tuve ninguna precaución al entrar pues me termino infectando todo y me di cuenta ya mucho tiempo después que el computador no me corría como debía.

¿Qué Harías?

R/ Siempre tratar de que cuando me conecte a una red que no sea la mia que me pregunte si quiero iniciar la conexión en modo seguro para así evitar este tipo de virus o cualquier otro tipo.

Paso #2

Recolección de Logs:

Logs del servidor de Correo Electrónico: En este punto de se debe de buscar los intentos de inicio de sesión fallidos o inusuales, También los envíos masivos de correos desde no autorizadas o fuera de horarios normal.

Logs del Sistema de Bases de Datos: Deberíamos identificar consultas inusuales o que accedan a gran volumen de datos de esta manera también debemos tener mucho cuidado y estar pendiente no solo de eso si no también a modificaciones no programadas en estructuras de tables o privilegios de usuario.

Logs de Seguridad: Tenemos que revisar y tener en cuenta la detección de malware o rensomware por parte del antivirus o EDR, así mismo estar muy pendiente y tener cuidado en que sitio o que archivo estamos o vamos a descargar en nuestro pc.

Análisis de la Actividad Maliciosa:

¿Qué análisis se debe realizar en los logs para buscar patrones inusuales?

R/ Aquí podemos realizar distintos análisis tales como un acceso fuera del horario laboral, inicio de sesión desde ubicaciones geográficas no registradas o inusuales así mismo las IPs desconocidas, Podemos también tener en cuenta también unos cambios en la configuración y actividades inusuales en base de datos.

¿Qué herramientas de análisis se podrían utilizar para los logs?

R/ Podemos utilizar las siguientes: Malwarebytes, Kaspersky Virus Removal Tool, Microsoft Defender.

Paso #3

¿Qué se debe realizar cuando se identifican los sistemas comprometidos?

R/ **Aislamiento inmediato del sistema infectado**
El gusano puede propagarse rápidamente a través de la red. Se debe desconectar el equipo afectado para frenar la infección.

Captura y análisis de logs y tráfico de red
Ver registros de actividad para identificar cuándo y cómo se inició la propagación. Herramientas como **Wireshark** pueden ayudar a rastrear el movimiento del gusano.

Registro del incidente
Documentar: IP del sistema, usuario activo, hora de la infección, nombre del gusano si se conoce, y si otros equipos presentan síntomas.

Revisión de sistemas interconectados

- Verificar servidores, terminales y otros dispositivos en la misma red local (LAN).
- Comprobar logs de red, DNS y firewall para detectar intentos de conexión a otros dispositivos.
- Evaluar si el gusano ha aprovechado vulnerabilidades comunes (puertos abiertos, credenciales débiles) para moverse lateralmente.

Evaluación del impacto en infraestructura crítica

Identificar si los equipos infectados forman parte de servicios como:

- Controladores de dominio
- Bases de datos principales
- Servidores de correo o archivos compartidos

Determinar si servicios críticos han sido interrumpidos o corrompidos.

¿Qué se debe tener en cuenta para evaluar el impacto en la disponibilidad, integridad y confidencialidad?

R/ La **disponibilidad** se ve afectada por los gusanos cuando saturan la red y consumen recursos del sistema, provocando lentitud o caída de servicios como correo, bases de datos o archivos compartidos.

R/ La **integridad** puede comprometerse si el gusano modifica archivos del sistema o configuraciones, generando errores, pérdida de datos o funcionamiento anómalo.

R/ La **confidencialidad** está en riesgo cuando el gusano recopila y envía información sensible, como contraseñas o documentos privados, a servidores externos controlados por atacantes.

Resultado Esperado

- **Identificación completa del alcance de la infección** en la red.
- **Clasificación del impacto** en términos de:
    - Disponibilidad: interrupción de servicios.
    - Integridad: modificación de datos o configuraciones.
    - Confidencialidad: posible fuga de información.
- **Base para tomar decisiones** sobre contención, erradicación y recuperación.

Paso #4

Restauración desde Copias de Seguridad

- Verificar que las copias de seguridad no estén infectadas por el gusano. Si se sospecha que el gusano ya estaba presente en los sistemas de respaldo, restaurar solo los archivos o configuraciones no comprometidas.
- Restaurar los sistemas afectados a un punto anterior a la infección, asegurándose de que los sistemas estén completamente libres del gusano antes de la restauración.
- Priorizar la recuperación de sistemas críticos como servidores de correo electrónico, bases de datos y sistemas de autenticación, ya que los gusanos suelen propagarse rápidamente a través de estos servicios.
- Si las copias de seguridad están comprometidas, realizar una reinstalación limpia de los sistemas desde imágenes seguras.

Monitoreo y Validación

- Realizar un análisis exhaustivo de los sistemas restaurados con herramientas especializadas en la detección de gusanos, como **Malwarebytes** o **ESET**.
- Monitorear el tráfico de red para detectar cualquier intento de propagación del gusano a través de puertos abiertos o vulnerabilidades explotadas por el malware.
- Validar que los archivos y bases de datos restaurados sean íntegros y no hayan sido alterados por el gusano, especialmente los archivos críticos para la operación.
- Asegurarse de que todos los servicios se reanuden correctamente, sin anomalías, y realizar pruebas de funcionamiento antes de volver a operar a plena capacidad.

Transparencia: ¿Qué se debe realizar?

R/ Informar a las partes clave de la organización:
Notificar a la alta dirección, el equipo de TI, y los responsables de la seguridad cibernética sobre la naturaleza del ataque, la magnitud de la infección y las medidas inmediatas que se han tomado. Es esencial mantenerlos al tanto de la situación para coordinar una respuesta rápida y eficaz.

Comunicar a los empleados afectados:
Informar a los empleados sobre los problemas de seguridad y cómo pueden evitar ser afectados por el gusano. Si es necesario, proporcionar instrucciones claras sobre cómo cambiar contraseñas o evitar comportamientos riesgosos mientras se resuelve el incidente.

Informar a los clientes y partes externas:
Si el gusano ha comprometido datos sensibles de clientes o ha afectado la disponibilidad de servicios, se debe informar a los clientes afectados. Esta comunicación debe ser clara, sincera y detallar las medidas que la empresa está tomando para resolver el problema.

Detallar las siguientes etapas:
Explicar las próximas acciones a tomar, como la restauración de sistemas, la validación de la eliminación del gusano, el monitoreo continuo y la mejora de las defensas para prevenir futuros incidentes. Asegurar que todos los involucrados comprendan los plazos y el seguimiento del incidente.