Práctica de laboratorio: Manejo de incidentes

Objetivos

Aplique todo lo que sabe sobre procedimientos para el manejo de seguridad para formular preguntas sobre determinados escenarios de incidentes.

Aspectos básicos / situación

La respuesta a ante incidentes de seguridad informática se ha convertido en un componente vital de cualquier organización. El proceso para manejar un incidente de seguridad puede ser complicado e implicar a muchos grupos diferentes. Una organización debe tener estándares para responder ante incidentes. Estos estándares deben ser políticas, procedimientos y listas de comprobación. Para responder correctamente a un incidente de seguridad, el analista debe estar capacitado para saber qué hacer, y también tiene que seguir todas las pautas estipuladas por la organización. Hay muchos recursos disponibles para ayudar a las organizaciones a crear y mantener una directiva de gestión de respuestas a incidentes del equipo. La publicación especial 800-61r2 de NIST se cita específicamente en los temas del examen Understanding Cybersecurity Operations Fundamentals (200-201 CBROPS).

Instrucciones

Situación 1: Infestación por gusanos y agentes de Denegación Distribuida de Servicio (Distributed Denial of Service, DDoS)

Estudie el siguiente escenario para analizar y determinar las preguntas sobre el manejo de la respuesta ante incidentes que se deberían formular en cada etapa del proceso de respuesta ante incidentes. Considere los detalles de la organización y el CSIRC cuando formulen sus preguntas.

Este escenario es una firma de inversiones pequeña y familiar. La organización tiene solo una sede y menos de 100 empleados. Es martes por la mañana y se libera un gusano nuevo; se propaga por medios extraíbles, y se puede copiar a sí mismo en recursos compartidos de Windows. Cuando el gusano infecta a un host, instala un agente de DDoS. Solo hubo firmas de antivirus disponibles varias horas después de que el gusano comenzara a propagarse. La organización ya había sufrido infecciones masivas.

La firma de inversiones ha contratado a un pequeño grupo de expertos en seguridad que suelen utilizar el modelo diamante para el manejo de incidentes de seguridad.

Preparación:

Detección y análisis:

Contención, erradicación y recuperación:

Actividad posterior al incidente:

Situación 2: Acceso no autorizado a registros de nómina

Estudie el siguiente escenario. Analice y determinen las preguntas sobre el manejo de la respuesta ante incidentes que se deberían formular en cada etapa del proceso de respuesta ante incidentes. Considere los detalles de la organización y el CSIRC cuando formulen sus preguntas.

Este escenario se trata de un hospital de mediana magnitud con varios consultorios y servicios médicos externos. La organización tiene decenas de sedes y más de 5000 empleados. Debido al tamaño de la organización, han adoptado un modelo CISRC con equipos distribuidos de respuesta ante incidentes. También tienen un equipo de coordinación que controla a los CSIRT y les ayuda a comunicarse entre sí.

Son las últimas horas de la tarde de un miércoles, el equipo de seguridad física de la organización recibe una llamada de una administradora de nómina que vio salir de su oficina a un desconocido, correr por el pasillo y salir del edificio. La administradora se había alejado de su estación de trabajo solo durante unos pocos minutos y la había dejado desbloqueada. El programa de nóminas sigue con la sesión abierta y en el menú principal, tal como ella lo había dejado, pero cree que han movido el mouse. Se le ha solicitado al equipo de respuesta ante incidentes que reúna evidencia relacionada con el incidente y determine qué medidas se deben tomar.

Los equipos de seguridad ponen en práctica el modelo de la cadena de eliminación y saben utilizar la base de datos VERIS. A modo de nivel de protección adicional, han tercerizado parcialmente el personal a una MSSP para tener monitoreo las 24 horas del día, los 7 días de la semana.

Preparación:

Detección y análisis:

Contención, erradicación y recuperación:

Actividad posterior al incidente: