Reporte Incidente: Ping Flood ICMP Attack 2024-05-13 #3  
Globe Sistemas - Av Libertador Jardin America

Descripción General del Reporte

| **Parte 1: Resumen del problema encontrado en el registro de tráfico DNS e ICMP.** | |
| --- | --- |
| El protocolo UDP revela que:  Esto se basa en los resultados del análisis de la red, que muestran que la respuesta de eco ICMP devolvió el mensaje de error:  El puerto indicado en el mensaje de error se utiliza para:  El problema más probable es: | |
|

| **Parte 2: Explique su análisis de los datos y proporcione al menos una causa del incidente.** |
| --- |
| Hora en que ocurrió el incidente:  Explique cómo el equipo de TI se enteró del incidente:  Explique las acciones tomadas por el departamento de TI para investigar el incidente:  Tenga en cuenta los hallazgos clave de la investigación del departamento de TI (es decir, detalles relacionados con el puerto afectado, el servidor DNS, etc.):  Tenga en cuenta una causa probable del incidente: |

| **Parte 1** | | |
| --- | --- | --- |
| **Proporcionar un resumen del problema encontrado en el registro de tráfico DNS e ICMP.** | | **Explicación** |
| **A** | Como parte del protocolo DNS, el protocolo UDP se utilizó para contactar al servidor DNS y recuperar la dirección IP del nombre de dominio globesistemas.com.  El protocolo ICMP se utilizó para responder con un mensaje de error, indicando problemas para contactar con el servidor DNS. | **Incluya un breve resumen del análisis del registro de tcpdump e identifique qué protocolos se utilizaron para el tráfico de la red.**  El escenario resume el problema e identifica los protocolos utilizados.  El escenario: “Para cargar la página web, su navegador primero envía una consulta a un servidor DNS a través del protocolo UDP para recuperar la dirección IP del nombre de dominio del sitio web; esto es parte del protocolo DNS...  El analizador muestra que cuando envía paquetes UDP al servidor DNS, recibe paquetes ICMP que contienen el mensaje de error: "puerto udp 53 inalcanzable". |
| **B** | El mensaje UDP que va desde su navegador al servidor DNS se muestra en las dos primeras líneas de cada evento de registro.  La respuesta de error ICMP del servidor DNS a su navegador se muestra en la tercera y cuarta líneas de cada evento de registro con el mensaje de error "puerto udp 53 inalcanzable".  Dado que el puerto 53 está asociado con el tráfico del protocolo DNS, sabemos que se trata de un problema con el servidor DNS.  Los problemas con la ejecución del protocolo DNS son aún más evidentes porque el signo más después del número de identificación de la consulta 35084 indica indicadores con el mensaje UDP y la letra "A?" .  El símbolo indica banderas con actuación Operaciones del protocolo DNS. | **Proporcionar algunos detalles sobre lo que se indicó en el registro.**  El primer y segundo paso de la sección del escenario indican que realizó un análisis de red utilizando tcpdump, que paquetes UDP grabados desde su computadora de origen a la dirección IP y al puerto del servidor DNS (203.0.113.2.dominio).  También registró las respuestas de error ICMP del servidor DNS a su computadora. con el mensaje de error "puerto udp 53 inalcanzable".  Mencionamos en el sexto paso que “El puerto 53 es un puerto para el servicio DNS”, lo que significa que se trata de un problema con el servidor DNS.  Incluimos más señales de problemas con el rendimiento del DNS en el quinto paso del escenario”,  El signo más después del número de identificación de la consulta indica que hay indicadores asociados con el mensaje UDP.  ¿La A?" indica un indicador asociado con la solicitud DNS de un registro A, donde un registro A asigna un nombre de dominio a una dirección IP”. |
| **C** | Debido al mensaje de respuesta de error ICMP sobre el puerto 53, es muy probable que el servidor DNS no responda.  Esta suposición se ve respaldada aún más por los indicadores asociados con el mensaje UDP saliente y la recuperación del nombre de dominio. | **Interpretar los problemas encontrados en el registro.**  La sección Escenario (o una búsqueda rápida en Internet para “puerto 53”) mostrará que este número de puerto se usa comúnmente para DNS protocolo de comunicaciones.  Dado que el puerto 53 es inalcanzable y ese puerto se usa comúnmente para las comunicaciones del servidor DNS, puede concluir que el servidor DNS es inalcanzable o "no responde".  Esto podría deberse, por ejemplo, a un ataque DoS contra el servidor DNS. |

| **Parte 2** | | |
| --- | --- | --- |
| **Explique su análisis de los datos y proporcione al menos una causa del incidente.** | | **Explicación** |
| **A** | El hecho ocurrió hoy a las 13:24 horas. | **Indique cuándo se informó el problema por primera vez.**  Esta información se obtuvo de las marcas de fecha y hora del archivo de registro. En el registro, esta es la primera secuencia de números que se muestra: 13:24:32.192571.  Esto muestra la hora 1:24 p. m., 32,192571 segundos, con la hora en formato de 24 horas.  El escenario indica que este evento ocurrió hoy. |
| **B** | Los clientes notificaron a la organización que recibieron el mensaje "puerto de destino inalcanzable" cuando intentaron visitar el sitio web globesistemas.com. | **Proporcione el escenario, los eventos y los síntomas identificados cuando se informó el evento por primera vez.**  El escenario establece que un puñado de clientes se comunicaron con su empresa para informar que no podían acceder al sitio web de la empresa y vieron el error "puerto de destino inalcanzable" después de esperar a que se cargará la página. |
| **C** | El equipo de ciberseguridad que brinda servicios de TI a la organización de su cliente está investigando actualmente el problema para que los clientes puedan acceder al sitio web nuevamente. | **Explique el estado actual del problema.**  El escenario establece que "este incidente, mientras tanto, está siendo manejado por ingenieros de seguridad después de que el analista haya informado del problema a su supervisor”. |
| **D** | En nuestra investigación del problema, realizamos pruebas de detección de paquetes utilizando tcpdump.  En el archivo de registro resultante, encontramos que no se podía acceder al puerto DNS 53. | **Describe la información descubierta al investigar el problema hasta este momento.**  Proporciona un resumen conciso de lo que hizo para investigar el problema.  El escenario dice: Se Visita el sitio web y también se recibe el error "puerto de destino inalcanzable".  A continuación, se cargó la herramienta de análisis de red, tcpdump, y se carga la página web nuevamente. Esta vez, se reciben muchos paquetes en su analizador de red.  En el analizador, envía paquetes UDP y recibe una respuesta ICMP para regresar al host.  Los resultados contienen un mensaje de error: "Puerto udp 53 inalcanzable". |
| **E** | El siguiente paso es identificar si el servidor DNS está inactivo o si el firewall bloquea el tráfico al puerto 53. | **Enumere los siguientes pasos para solucionar problemas y resolver el problema.**  El siguiente paso en la solución de problemas es determinar si el servidor DNS no funciona correctamente.  Si el servidor DNS está bien, el equipo debe verificar la configuración del firewall para ver si alguien cambió la configuración para bloquear el tráfico de red en el puerto 53.  Los firewalls ofrecen la capacidad de bloquear el tráfico de red en puertos específicos. El bloqueo de puertos se puede utilizar para detener o prevenir un ataque. |
| **F** | El servidor DNS puede estar inactivo debido a un ataque de denegación de servicio exitoso o a una mala configuración. | **Proporcionar la causa raíz sospechada del problema.**  Anteriormente, conoció varios tipos de ataques de denegación de servicio (DoS).  El objetivo de un ataque DoS es enviar una avalancha de información a un dispositivo de red, como un servidor DNS, para bloquearlo o impedir que responda al tráfico legítimo de la red.  Es posible que un atacante haya desactivado el servidor DNS con un ataque DoS.  Alternativamente, alguien de su equipo podría haber realizado un cambio de configuración en el firewall que bloqueó el puerto 53. |