GUÍA PARA CONTRARRESTAR INCIDENTES DE

ESCANEO SMB

SMB (Server Message Block) es un protocolo utilizado principalmente en sistemas Windows para compartir archivos, impresoras y otros recursos dentro de una red.

El escaneo SMB consiste en identificar dispositivos que tienen habilitado este servicio, generalmente a través de los puertos 445 y 139. Aunque puede utilizarse de forma legítima para tareas administrativas, también puede ser aprovechado por atacantes para detectar sistemas vulnerables y preparar posibles ataques informáticos.

¿CÓMO FUNCIONAN LOS ATAQUES DE RETRANSMISIÓN SMB?

* El atacante identifica equipos con el servicio SMB habilitado mediante escaneo de red.
* Intercepta la comunicación entre el usuario y el servidor utilizando técnicas como Man-in-the- Middle (MitM).
* Captura la solicitud de autenticación SMB enviada por el usuario.
* Retransmite las credenciales capturadas hacia otro servidor SMB.
* El servidor objetivo valida la autenticación y concede acceso al atacante, quien se hace pasar por el usuario legítimo.

Nota: Man-in-the-Middle

(MitM) es una técnica de ataque en la que un actor malicioso intercepta la comunicación entre dos sistemas para capturar o manipular información sin ser detectado.

¿CUÁL ES EL OBJETIVO DE LOS ATAQUES DE RETRANSMISIÓN SMB?

Los ataques de retransmisión SMB tienen como objetivo permitir a los atacantes obtener acceso no autorizado a sistemas y redes sin necesidad de descifrar contraseñas. Una vez dentro de la infraestructura, pueden identificar otros equipos vulnerables, desplazarse lateralmente y comprometer más recursos de la red.

GUIA PARA CONTRARRESTAR INCIDENTES DE ESCANEO SMB

PASO 1

IDENTIFICAR ACTIVIDAD SMB SOSPECHOSA

- ***Revisar*** *conexiones al puerto TCP 445 y 139.*
- ***Detectar*** *múltiples intentos de autenticación SMB.*
- ***Verificar*** *alertas IDS/IPS relacionadas con SMB.*

PASO 2

ANALIZAR EL ORIGEN DEL ESCANEO

- ***Identificar*** *la dirección IP origen.*
- ***Determinar*** *si el tráfico proviene de un equipo interno o externo.*
- ***Revisar*** *logs de autenticación y eventos de red.*

PASO 3

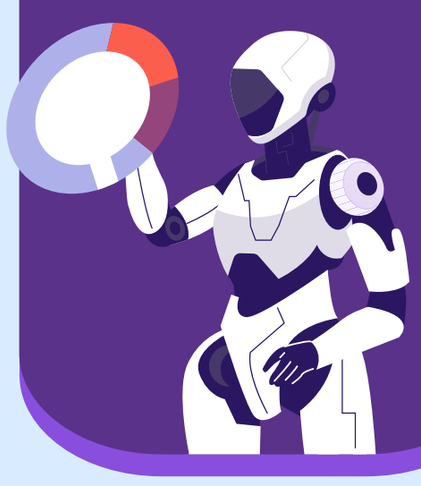
CONTENER LA ACTIVIDAD SOSPECHOSA

- ***Bloquear*** *temporalmente la IP origen.*
- ***Restringir*** *tráfico SMB innecesario.*
- ***Aislar*** *equipos comprometidos si es necesario.*

PASO 4

FORTALECER LA SEGURIDAD SMB

- ***Deshabilitar*** *SMBv1.*
- ***Habilitar*** *SMB Signing.*
- ***Restringir*** *acceso al puerto TCP 445.*
- ***Aplicar*** *segmentación de red.*



PASO 5

VERIFICAR POSIBLES AFECTACIONES

- ***Revisar*** *accesos no autorizados.*
- ***Analizar*** *intentos de movimiento lateral.*
- ***Verificar*** *recursos compartidos comprometidos.*

PASO 3

IMPLEMENTAR MONITOREO CONTINUO

- ***Supervisar*** *tráfico SMB constantemente.*
- ***Configurar*** *alertas de escaneo y autenticación sospechosa.*
- ***Mantener*** *actualizados sistemas y herramientas de seguridad.*

MEDIDAS PARA CONTRARRESTAR EL ESCANEO SMB

- Restringir el acceso al puerto TCP 445 únicamente a equipos autorizados.
- Bloquear conexiones SMB provenientes de redes externas o no confiables.
- Deshabilitar SMBv1 en todos los sistemas de la organización.
- Implementar segmentación de red para limitar el tráfico SMB entre equipos.
- Supervisar continuamente la red para detectar escaneos SMB sospechosos.
- Configurar reglas IDS/IPS para identificar intentos de enumeración SMB.
- Mantener sistemas operativos y servicios SMB actualizados.
- Limitar los recursos compartidos únicamente a usuarios autorizados.
- Aplicar políticas de autenticación seguras y control de accesos.
- Revisar periódicamente logs de autenticación y conexiones SMB inusuales.

ecucert
Centro de respuesta a incidentes informáticos del Ecuador

EL NUEVO ECUADOR