Ataques y defensas en WMI

1. Ejecución de comandos remotos

Una técnica común es utilizar WMI para ejecutar comandos en máquinas remotas. El siguiente script de PowerShell muestra cómo ejecutar un comando en una máquina remota utilizando WMI:

[crayon-6a9dbfa290c07665199586/]

Este script utiliza Invoke-WmiMethod para invocar el método Create del objeto Win32_Process, lo que permite ejecutar comandos.

2. Búsqueda de instancias de MOF maliciosas

Puedes buscar instancias de archivos MOF (Management Object Format) que podrían haber sido alterados o implantados por atacantes:

[crayon-6a9dbfa290c0e692203549/]

Estos comandos buscan en el namespace root\subscription objetos que puedan ser parte de la persistencia de un malware o un ataque.

3. Monitorización y registro de actividades de WMI

Para detectar posibles usos maliciosos de WMI, puedes configurar el registro de eventos de WMI:

[crayon-6a9dbfa290c11079157831/]

Estos comandos ajustan el registro en el sistema para capturar actividades de WMI y luego recuperar esos registros para

análisis.

4. Restringiendo acceso a WMI

Puedes restringir el acceso a WMI para mitigar el riesgo de ataques, ajustando los permisos mediante PowerShell:

[crayon-6a9dbfa290c12122861517/]