Limpie el acceso - Utilice la característica de la exploración de la red para detectar a los usuarios que intentan desviar los controles del agente

Contenido

Introducción

El acceso limpio de Cisco es una solución de cumplimiento de la política de seguridad que permite a los usuarios para satisfacer los requisitos del acceso a la red especificados por los administradores de la red. El acceso limpio de Cisco restringe el acceso a la red hasta que el usuario cumpla con los requisitos del acceso. El acceso limpio de Cisco también ayuda al usuario a cumplir con los requisitos con una aplicación de cliente fácil de usar que evalúe un sistema, detecte el incumplimiento, y ayude al usuario en la corrección para alcanzar la conformidad. Actualmente, se soporta este agente (aplicación de cliente) está disponible solamente para los sistemas operativos de Microsoft Windows que incluyen Windows 98, Windows yo, Windows 2000 Professional y Windows XP (casero y favorable – solamente la versión 32-bits del Pro).

Los usuarios malintencionados, que pudieron querer evitar la instalación del agente para evitar los controles de los requisitos de la conformidad, pueden modificar su sistema para presentar como sistema distinto de Windows. Este documento proporciona las sugerencias en cómo detectar a tales usuarios y potencialmente bloquear su acceso a la red.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Windows 98, Windows yo, Windows 2000 Professional y Windows XP (casero y favorable – solamente la versión 32-bits del Pro se soporta)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Solución

Además de las exploraciones y de la corrección basadas en el cliente, el acceso limpio de Cisco también proporciona los mecanismos para realizar las exploraciones Basadas en red en los sistemas y para proporcionar la corrección basada en web. Las exploraciones Basadas en red se utilizan sobre todo para los sistemas distintos de Windows. Sin embargo, las exploraciones no se limitan a los sistemas distintos de Windows.

Para utilizar la característica de la exploración de la red, el administrador de la red necesita descargar y instalar los enchufes requeridos para el escáner de vulnerabilidad del código abierto del Nessus en el servidor de acceso limpio de Cisco. Refiera a configurar la exploración de la red en el *dispositivo NAC de Cisco - la guía de instalación y configuración limpia del Access Manager, libera 4.1(2)* para la información sobre cómo descargar y instalar los enchufes del Nessus.

Usted puede utilizar los enchufes múltiples del Nessus en este escenario. Algunos de ellos son (esto es una lista no exhaustiva):

- **Enchufes para la identificación del sistema operativo** (por ejemplo, #11936 plug-in) — cuando usted ejecuta estos enchufes contra un sistema de destino, proporcionan el nombre detectado del sistema operativo como resultado de una exploración. Estos enchufes necesitan ser modificados para ser utilizado dentro del acceso limpio de Cisco. Específicamente, los enchufes necesitan ser modificados para volver un AGUJERO si el sistema operativo se analiza que no es un sistema operativo del no Windows. Por ejemplo, si el sistema Linux se analiza que resulta ser un Sistema Windows, después el enchufe debe volver un resultado del AGUJERO.
- **Enchufes para la análisis de puertos** (por ejemplo, nmap.nasl) — cuando usted ejecuta estos enchufes contra un sistema de destino, usted puede configurarlos para proporcionar una lista de puertos abiertos, los módulos de escucha, y así sucesivamente. Estos enchufes también tienen la capacidad de detectar qué sistema operativo se utiliza en el host con las técnicas tales como identificación por huellas digitales TCP. Usted necesita modificar estos enchufes igual que los enchufes para la identificación del sistema operativo. Necesitan volver un AGUJERO si el sistema operativo se analiza que no es un sistema operativo del no Windows. Específicamente, usted necesita modificar los enchufes para volver un AGUJERO si el sistema operativo previsto no es un sistema operativo del no Windows. Por ejemplo, si el sistema Linux se analiza que resulta ser un Sistema Windows, después el enchufe debe volver un resultado del AGUJERO.
- **Enchufes para obtener la información de los Sistemas Windows** (por ejemplo, el [SMB] del

bloque de mensaje del servidor - los enchufes relacionados y #10859 plug-in) — el razonamiento detrás de este acercamiento es que es bastante suficiente detectar si una máquina que pretende ser un host de Linux, host del mac, o cualquier otro sistema distinto de Windows, es realmente un Sistema Windows. La manera más fácil de hacer esto es habilitar algunos enchufes SMB-relacionados del Nessus, el id# específicamente plug-in 10859 (el SMB consigue el host SID). Este enchufe debe solamente los valores devueltos para los Sistemas Windows. Por lo tanto, si devuelve alguna información, puede ser concluido con seguridad que el sistema funciona con un sistema operativo Windows. Usted puede también utilizar los enchufes que recuperan la información de los Sistemas Windows que utilizan el NETBIOS. Si un sistema devuelve la información de NetBIOS, es probable ser un Sistema Windows.**Precaución:** Pudo haber falsos positivos tales como máquinas de Linux que funcionan con la samba.

Complete estos pasos para configurar un Access Manager limpio de Cisco para realizar una exploración de la red usando los enchufes del Nessus:

1. Abra la consola Web limpia del Access Manager de Cisco en un navegador y inicie sesión como administrador.
2. Seleccione el **acceso limpio > Network Scanner (Escáner de red)** acceder la página de configuración de la exploración.
3. Con el conjunto del papel al rol del usuario usted desea analizar, y el sistema operativo fijado a **todos**, selecciona el enchufe mencionado en los enchufes para obtener la información del elemento con viñetas de los Sistemas Windows dentro de este documento (por ejemplo, #10859).
4. Fije el “vulnerable si…” fijando **PARA AGUJEREAR, ADVIERTA, INFORMACIÓN** en la sección de las vulnerabilidades.
5. Inhabilite la exploración para los sistemas operativos Windows:Seleccione **WIN_ALL de la** lista desplegable del sistema operativo.Inhabilite la exploración para esta selección.

Resumen

Este documento proporciona un mecanismo para utilizar la característica limpia de la exploración de la red de acceso de Cisco para detectar a los usuarios que fingen utilizar un sistema distinto de Windows. Observe que pudo haber varios otros enchufes disponibles que pueden hacer un mejor trabajo en la detección de los sistemas operativos. Como un ejemplo, usando la herramienta de la exploración de la red del nmap, xprobe2 de la Sys-Seguridad, y así sucesivamente pudo caber sus necesidades mejor. También observe que la exploración de la red no pudo poder proporcionar los resultados confiables si la máquina del cliente funciona con un escudo de protección personal.

Notas

- El Nessus es una marca registrada de seguridad de la red sostenible.
- Usted necesita registrarse con la Seguridad sostenible para obtener los enchufes del Nessus.
- Cuando usted se modifica/los enchufes del autor, asegúrese de que usted sea obediente con los requisitos de la autorización y de la marca registrada para el Nessus y la seguridad de la red sostenible.

Información Relacionada

- Soporte de productos limpio del acceso de Cisco (dispositivo NAC)
- Soporte Técnico y Documentación - Cisco Systems