Clean Access - Utiliser la fonctionnalité d'analyse de réseau pour détecter les utilisateurs qui tentent de contourner les contrôles des agents

Contenu

Introduction

Cisco Clean Access est une solution de conformité de stratégie de sécurité qui permet à des utilisateurs de répondre à des exigences d'accès au réseau spécifiées par des administrateurs réseau. Cisco Clean Access limite l'accès au réseau jusqu'à ce que l'utilisateur se conforme aux conditions requises d'accès. Cisco Clean Access aide également l'utilisateur à se conformer aux conditions requises par une application cliente facile à utiliser qui évalue un système, détecte l'insoumission, et aide l'utilisateur dans la correction afin de réaliser la conformité. Actuellement, cet agent (application cliente) est disponible seulement pour les systèmes d'exploitation de Microsoft Windows qui incluent le Windows 98, le Windows je, le Windows 2000 Professional et le Windows XP (à la maison et pro – seulement la version 32-bits de pro est pris en charge).

Les utilisateurs malveillants, qui pourraient vouloir éviter l'installation d'agent afin d'éviter des contrôles de conformités aux réglementations, peuvent modifier leur système pour poser comme système de non-Windows. Ce document fournit des suggestions sur la façon dont détecter de tels utilisateurs et bloquer potentiellement leur accès au réseau.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Windows 98, Windows je, Windows 2000 Professional et Windows XP (à la maison et pro –

seulement la version 32-bits de pro est prise en charge)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Solution

En plus des balayages et de la correction basés sur client, Cisco Clean Access fournit également des mécanismes pour exécuter des balayages Fondé(e) sur le réseau sur des systèmes et pour fournir la correction basée sur le WEB. Les balayages Fondé(e) sur le réseau sont principalement utilisés pour des systèmes de non-Windows. Cependant, les balayages ne sont pas limités aux systèmes de non-Windows.

Afin d'utiliser la caractéristique de lecture de réseau, l'administrateur réseau doit le télécharger et installer les connexions requises pour le Nessus ouvrez le scanner de vulnérabilité de source sur le serveur de Cisco Clean Access. Référez-vous à configurer la lecture de réseau dans l'*appliance de Cisco NAC - le guide d'installation et de configuration de Clean Access Manager, libèrent 4.1(2)* pour des informations sur la façon télécharger et installer des connexions de Nessus.

Vous pouvez utiliser de plusieurs connexions de Nessus dans ce scénario. Certains d'entre eux sont (c'est une liste non exhaustive) :

- **Connexions pour l'identification du système d'exploitation** (par exemple, périphérique prêt à brancher #11936) — quand vous exécutez ces connexions contre un système cible, elles fournissent le nom du système d'exploitation détecté suite à un balayage. Ces connexions doivent être modifiées afin de pour être utilisées dans Cisco Clean Access. Spécifiquement, les connexions doivent être modifiées pour renvoyer un TROU si le système d'exploitation qui est balayé n'est pas un système d'exploitation de non-Windows. Par exemple, si le système Linux qui est balayé s'avère être un système Windows, puis le périphérique prêt à brancher devrait renvoyer un résultat de TROU.
- **Connexions pour la lecture de port** (par exemple, nmap.nasl) — quand vous exécutez ces connexions contre un système cible, vous pouvez les configurer pour fournir une liste de ports ouverts, des auditeurs, et ainsi de suite. Ces connexions ont également la capacité de détecter quel système d'exploitation est utilisé sur l'hôte par des techniques telles que la prise d'empreintes digitales de TCP. Vous devez modifier ces connexions de la même manière que les connexions pour l'identification du système d'exploitation. Ils doivent renvoyer un TROU si le système d'exploitation qui est balayé n'est pas un système d'exploitation de non-Windows. Spécifiquement, vous devez modifier les connexions pour renvoyer un TROU si le système d'exploitation prévu n'est pas un système d'exploitation de non-Windows. Par exemple, si le système Linux qui est balayé s'avère être un système Windows, puis le périphérique prêt à brancher devrait renvoyer un résultat de TROU.
- **Les connexions pour obtenir les informations des systèmes Windows** (par exemple, à connexions et à périphérique prêt à brancher liés #10859 de server message block [PME]) —

le raisonnement derrière cette approche est qu'il est assez suffisant de le détecter si un ordinateur qui prétend être un hôte de Linux, hôte de MAC, ou n'importe quel autre système de non-Windows, est réellement un système Windows. Le moyen le plus simple de faire ceci est d'activer quelques connexions liées à la PME de Nessus, l'id# spécifiquement embrochable 10859 (la PME obtiennent l'hôte SID). Ce périphérique prêt à brancher devrait seulement renvoyer des valeurs pour des systèmes Windows. Par conséquent, s'il renvoie n'importe quelles informations, il peut sans risque conclure que le système exploite un système d'exploitation Windows. Vous pouvez également utiliser les connexions qui récupèrent les informations des systèmes Windows qui utilisent NETBIOS. Si un système renvoie les informations de NETBIOS, il est susceptible d'être un système Windows.**Attention :** Il pourrait y avoir des faux positifs tels que les machines Linux qui exécutent la samba.

Terminez-vous ces étapes afin de configurer un gestionnaire de Cisco Clean Access pour exécuter un balayage de réseau utilisant les connexions de Nessus :

1. Ouvrez la console Web de gestionnaire de Cisco Clean Access dans un navigateur et une procédure de connexion en tant qu'administrateur.
2. **Le scanner** choisi de **Clean Access > de réseau** pour accéder au balayage a installé la page.
3. Avec le positionnement de rôle au rôle de l'utilisateur vous souhaitez balayer, et le système d'exploitation réglé à **tous**, sélectionnent le périphérique prêt à brancher mentionné dans les connexions pour obtenir les informations de l'élément à puces de systèmes Windows dans ce document (par exemple, #10859).
4. Placez le « vulnérable si… » en plaçant **POUR TROUER, AVERTISSEZ, les INFORMATIONS** dans la section de vulnérabilités.
5. Désactivez le balayage pour des systèmes d'exploitation Windows :**WIN_ALL** choisi de la liste déroulante du système d'exploitation.Désactivez le balayage pour cette sélection.

Résumé

Ce document fournit un mécanisme pour employer la caractéristique de lecture de réseau de Cisco Clean Access pour détecter les utilisateurs qui feignent pour utiliser un système de non-Windows. Notez qu'il pourrait y avoir plusieurs autres connexions disponibles qui peuvent réaliser un meilleur travail à détecter des systèmes d'exploitation. Comme exemple, utilisant l'outil de lecture de réseau de nmap, xprobe2 de Système-Sécurité, et ainsi de suite pourrait adapter vos besoins mieux. Notez également que la lecture de réseau ne pourrait pas pouvoir fournir des résultats fiables si la machine cliente exécute un pare-feu personnel.

Notes

- Nessus est une marque déposée de sécurité des réseaux défendable.
- Vous devez s'inscrire à la Sécurité défendable afin d'obtenir des connexions de Nessus.
- Quand vous modifie/connexions d'auteur, assurez-vous que vous êtes conforme avec les conditions requises d'autorisation et de marque pour Nessus et sécurité des réseaux défendable.

Informations connexes

- Support produit de Cisco Clean Access (appliance NAC)

- Support et documentation techniques - Cisco Systems