Limpe o acesso - Use a característica da exploração da rede para detectar os usuários que tentam contornear verificações do agente

Índice

Introdução

O acesso limpo de Cisco é uma solução de conformidade da política de segurança que permita usuários de satisfazer as exigências do acesso de rede especificadas por administradores de rede. O acesso limpo de Cisco restringe o acesso à rede até que o usuário siga com as exigências do acesso. O acesso limpo de Cisco igualmente ajuda o usuário a seguir com as exigências com um aplicativo do cliente fácil de usar que avalie um sistema, detecte a NON-conformidade, e ajude ao usuário na remediação para conseguir a conformidade. Atualmente, este agente (aplicativo do cliente) está disponível somente para os sistemas operacionais de Microsoft Windows que incluem Windows 98, Windows mim, Windows 2000 Professional e Windows XP (home e PRO – somente a versão 32-bits do PRO é apoiado).

Os usuários maliciosos, que puderam querer evitar a instalação de agente a fim evitar verificações das exigências da conformidade, podem alterar seu sistema para levantar como um sistema diferente do Windows. Este documento fornece sugestões em como detectar tais usuários e obstruir potencialmente seu acesso à rede.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Windows 98, Windows mim, Windows 2000 Professional e Windows XP (home e PRO –

somente a versão 32-bits do PRO é apoiada)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Solução

Além do que as varreduras e a remediação cliente-baseadas, o acesso limpo de Cisco igualmente fornece mecanismos para executar varreduras Com base na rede em sistemas e para fornecer a remediação com base na Web. As varreduras Com base na rede são usadas primeiramente para sistemas diferentes do Windows. Contudo, as varreduras não são limitadas aos sistemas diferentes do Windows.

A fim usar a característica da exploração da rede, o administrador de rede precisa de transferir e instalar os encaixes requerido para o scanner de vulnerabilidade da aberta de Nessus no servidor de acesso limpo de Cisco. Refira configurar a exploração da rede na *ferramenta NAC de Cisco - o Guia de Instalação e Configuração limpo do Access Manager, libera 4.1(2)* para obter informações sobre de como transferir e instalar plugin Nessus.

Você pode usar plugin Nessus múltiplos nesta encenação. Alguns deles são (esta é uma lista não-abrangente):

- **Encaixes para a identificação do sistema operacional** (por exemplo, #11936 de encaixe) — quando você executar estes encaixes contra um sistema de destino, fornecem o nome detectado do sistema operacional como consequência de uma varredura. Estes encaixes precisam de ser alterados a fim ser usado dentro do acesso limpo de Cisco. Especificamente, os encaixes precisam de ser alterados para retornar um FURO se o sistema operacional que está feito a varredura não é um sistema operacional não-Windows. Por exemplo, se o sistema Linux que está feito a varredura despeja ser um sistema Windows, a seguir o encaixe deve retornar um resultado do FURO.
- **Encaixes para a exploração da porta** (por exemplo, nmap.nasl) — quando você executar estes encaixes contra um sistema de destino, você pode configurar-los para fornecer uma lista de portas aberta, ouvintes, e assim por diante. Estes encaixes igualmente têm a capacidade para detectar que sistema operacional é usado no host com as técnicas tais como o fingerprinting TCP. Você precisa de alterar da mesma forma estes encaixes como os encaixes para a identificação do sistema operacional. Precisam de retornar um FURO se o sistema operacional que está feito a varredura não é um sistema operacional não-Windows. Especificamente, você precisa de alterar os encaixes para retornar um FURO se o sistema operacional previsto não é um sistema operacional não-Windows. Por exemplo, se o sistema Linux que está feito a varredura despeja ser um sistema Windows, a seguir o encaixe deve retornar um resultado do FURO.
- **Encaixes para obter a informação dos sistemas Windows** (por exemplo, o [SMB] do bloqueio de mensagem de servidor - encaixes relacionados e #10859 de encaixe) — o raciocínio atrás

desta aproximação é que é suficiente bastante detectar se uma máquina que os sentidos ser um host de Linux, host do Mac, ou todo o outro sistema diferente do Windows, sejam realmente um sistema Windows. A maneira a mais fácil de fazer isto é permitir alguns plugin Nessus SMB-relacionados, o id# especificamente de encaixe 10859 (o SMB obtém o host SID). Este encaixe deve somente retornar valores para sistemas Windows. Daqui, se retorna alguma informação, pode-se com segurança concluir que o sistema executa um sistema operacional de Windows. Você pode igualmente usar os encaixes que recuperam a informação dos sistemas Windows que usam NETBIOS. Se um sistema retorna a informação de NetBios, é provável ser um sistema Windows.**Caution**: Pôde haver falsos positivos tais como as máquinas de Linux que executam o samba.

Termine estas etapas a fim configurar um Access Manager limpo de Cisco para executar uma varredura da rede usando os plugin Nessus:

1. Abra o console de web limpo do Access Manager de Cisco em um navegador e em um início de uma sessão como um administrador.
2. Selecione o **acesso limpo > o scanner de rede** para alcançar a página de instalação da varredura.
3. Com o grupo do papel ao papel de usuário você deseja fazer a varredura, e o sistema operacional ajustado a **tudo**, seleciona o encaixe mencionado nos encaixes para obter a informação do item com boletim dos sistemas Windows dentro deste documento (por exemplo, #10859).
4. Ajuste o “vulnerável se…” ajustando-se **PARA FURAR, ADVIRTA, INFORMAÇÃO na** seção das vulnerabilidades.
5. Desabilite a varredura para sistemas operacionais de Windows:Selecione **WIN_ALL da** lista de drop-down do sistema operacional.Desabilite a varredura para esta seleção.

Resumo

Este documento fornece um mecanismo para usar a característica limpa da exploração da rede de acesso de Cisco para detectar os usuários que fingem usar um sistema diferente do Windows. Note que pôde haver diversos outros encaixes disponíveis que podem fazer um trabalho melhor em detectar sistemas operacionais. Como um exemplo, usando a ferramenta da exploração da rede do nmap, xprobe2 da SYS-Segurança, e assim por diante pôde caber suas necessidades melhor. Igualmente note que a exploração da rede não pôde poder fornecer resultados seguros se a máquina cliente executa um firewall pessoal.

Notas

- Nessus é uma marca registrada de segurança de rede sustentável.
- Você precisa de registrar-se com Segurança sustentável a fim obter plugin Nessus.
- Quando você altera/encaixes do autor, assegure-se de que você esteja complacente com as exigências licenciar e de marca registrada para Nessus e a segurança de rede sustentável.

Informações Relacionadas

- Sustentação do produto limpa do acesso de Cisco (ferramenta NAC)
- Suporte Técnico e Documentação - Cisco Systems