Clean Access -使用网络扫描功能发现尝试绕过代理检查的用户

目录

简介

思科Clean Access是使用户满足网络管理员指定的网络访问要求的安全策略标准解决方案。思科Clean Access限制对网络的访问，直到用户符合访问需求。思科Clean Access也帮助用户服从需求通过估计一个系统，检测不顺从，并且帮助修正的用户以便达到标准的一个易用客户端应用。目前，此代理程序(客户端应用)为包括Windows 98、Windows我， Windows 2000 Professional和Windows XP操作系统的Microsoft Windows是仅可用的(家庭和亲支持)仅的32 BITS版本赞成。

有恶意的用户，也许要避免代理程序安装为了避免标准需求检查，能修改他们的系统摆在作为非Windows系统。本文提供建议关于怎样检测这样用户和潜在阻止他们的对网络的访问。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件版本：

- Windows 98、Windows我， Windows 2000 Professional和Windows XP (家庭和亲支持仅32 BITS版本赞成)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

解决方案

除基于客户的扫瞄和修正之外，思科Clean Access也提供机制执行在系统的基于网络扫瞄和提供基于Web的修正。基于网络扫瞄主要使用非Windows系统。然而，扫瞄对非Windows系统没有被限制。

为了使用网络扫描功能，网络管理员需要下载和安装Nessus开放源漏洞扫描仪的需要的插件在思科Clean Access服务器。参考配置在*Cisco NAC设备的*网络扫描-关于如何下载和安装Nessus插件的信息， *Clean Access管理器安装和配置指南，发布4.1(2)*。

您在此方案能使用多个Nessus插件。有些是(这是一不详尽的列表) ：

- **操作系统的识别的插件**(例如， plug-in #11936) —，当您执行这些插件目标系统，由于扫描，他们提供检测的操作系统名称。需要修改这些插件为了在思科Clean Access内使用。特别地，需要修改插件返回孔，如果被扫描的操作系统不是一个非Windows操作系统。例如，如果被扫描的Linux系统结果是windows系统，然后plug-in应该返回孔结果。
- **端口扫瞄的插件**(例如， nmap.nasl) —，当您执行这些插件目标系统，您能配置他们提供开放端口列表，监听程序，等等。这些插件也有能力检测哪个操作系统在主机使用通过技术例如TCP指纹识别。您需要以与操作系统的识别的插件相似的方式修改这些插件。他们需要归还孔，如果被扫描的操作系统不是一个非Windows操作系统。特别地，如果预计操作系统不是一个非Windows操作系统，您需要修改插件归还孔。例如，如果被扫描的Linux系统结果是windows系统，然后plug-in应该返回孔结果。
- **得到信息的插件从Windows系统**(例如，服务器消息块[SMB]有关的插件和plug-in #10859) —在此方法后的推理是检测声称是Linux主机、Mac主机，或者其他非Windows系统的是足够满足的计算机，是否实际上是windows系统。要执行此的简便的方法是启用一些SMB-related Nessus插件，特别地插件id- 10859 (SMB获得主机SID)。此plug-in应该只返回windows系统的值。因此，如果返回任何信息，可以安全推断系统运行Windows操作系统。您能也使用从windows系统恢复信息使用NETBIOS的插件。如果系统返回NETBIOS信息，是windows系统可能的。**警告：** 也许有错误肯定例如运行桑巴的Linux机器。

使用Nessus插件，完成这些步骤为了配置思科Clean Access管理器执行网络扫描：

1. 打开在浏览器和登录的思科Clean Access管理器Web控制台作为管理员。
2. 选择**Clean Access >**访问扫描设置页的**网络扫描仪**。
3. 角色设置为用户角色您希望扫描，并且操作系统设置对**所有**，选择在插件提及的plug-in从在本文内的Windows系统打弹号项目得到信息(例如， #10859)。
4. 设置‘易受攻击，如果…’设置**钻孔，请警告，**在漏洞部分的**INFO**。
5. 禁用Windows操作系统的扫描：选择从操作系统的下拉列表的**WIN_ALL**。禁用此选择的扫描。

摘要

本文提供一机制使用思科Clean Access网络扫描功能检测假装使用非Windows系统的用户。注意也许能做一个更加好的工作在检测操作系统的几其他插件取得到。为例，使用nmap网络扫描工具，从Sys-security的xprobe2，等等也许适合更加好您的需要。并且请注意网络扫描也许不能提供可靠结果客户端机器是否机器运行个人防火墙。

备注

- Nessus是站得住脚的网络安全注册商标。
- 您需要向站得住脚的安全登记为了获取Nessus插件。
- 当您修改/作者插件时，请保证您与Nessus和站得住脚的网络安全的许可授权的和商标需求是兼容的。

相关信息

- 思科Clean Access (NAC设备)产品支持
- 技术支持和文档 - Cisco Systems