Чистый Доступ - использует функцию просмотра сети, чтобы обнаружить пользователей, пытающихся обойти проверки агента

Содержание

Введение

Cisco Clean Access является решением, отвечающим требованиям политики политики безопасности, которое позволяет пользователям удовлетворить требования доступа к сети, заданные администраторами сети. Cisco Clean Access ограничивает доступ к сети, пока пользователь не соответствует требованиям доступа. Cisco Clean Access также помогает пользователю соответствовать требованиям через простое в использовании клиентское приложение, которое оценивает систему, обнаруживает несоблюдение и помогает пользователю в исправлении, чтобы достигнуть соответствия. В настоящее время этот агент (клиентское приложение) доступен только для операционных систем Microsoft Windows, которые включают Windows 98, Windows Me, Windows 2000 Professional и Windows XP (и Дом и Pro – только 32 32-х битных версии Pro поддерживаются).

Вредоносные пользователи, которые могли бы хотеть избежать установки агента во избежание проверок требований соответствия, могут модифицировать свою систему для изображения из себя отличной от Windows система. Этот документ предоставляет предложения о том, как обнаружить таких пользователей и потенциально блокировать их доступ к сети.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- Windows 98, Windows Me, Windows 2000 Professional и Windows XP (и Дом и Pro – только 32 32-х битных версии Pro поддерживаются),

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Решение

В дополнение к основанным на клиенте просмотрам и исправлению, Cisco Clean Access также предоставляет механизмы, чтобы выполнить сетевые просмотры в системах и предоставить находящееся на web исправление. Сетевые просмотры прежде всего используются для отличных от Windows система. Однако просмотры не ограничены отличными от Windows система.

Для использования функции Сканирования Сети администратор сети должен загрузить и установить обязательные подключаемые модули для сканнера уязвимости открытого источника Nessus на сервере Cisco Clean Access. См. Настройку сети, Просматривающей в *устройстве Cisco NAC - Чистят Руководство по установке и конфигурированию Access Manager, Выпуск 4.1 (2)* для получения информации о том, как загрузить и установить подключения Nessus.

Можно использовать множественные подключения Nessus в этом сценарии. Некоторые из них (это - неполный список):

- **Плагины для Идентификации Операционной системы** (например, плагин #11936) — Когда вы выполняете эти плагины против целевой системы, они предоставляют обнаруженное название операционной системы как результат просмотра. Эти плагины должны модифицироваться, чтобы использоваться в Cisco Clean Access. В частности плагины должны модифицироваться для возврата ДЫРЫ, если операционная система, которая просмотрена, не является операционной системой не-Windows. Например, если Система Linux, которая просмотрена, оказывается, Система Windows, тогда плагин должен возвратить результат ДЫРЫ.
- **Плагины для Сканирования портов** (например, nmap.nasl) — при выполнении этих плагинов против целевой системы можно настроить их для обеспечения списка открытых портов, слушателей, и т.д. Эти плагины также имеют способность обнаружить, какая операционная система используется на хосте через способы, такие как снятие отпечатков пальцев TCP. Необходимо модифицировать эти плагины таким же образом как плагины для идентификации операционной системы. Они должны возвратить ДЫРУ, если операционная система, которая просмотрена, не является операционной системой не-Windows. В частности, если ожидаемая операционная система не является

операционной системой не-Windows, необходимо модифицировать плагины для возврата ДЫРЫ. Например, если Система Linux, которая просмотрена, оказывается, Система Windows, тогда плагин должен возвратить результат ДЫРЫ.
- **Плагины для Получения информации из Систем Windows** (например, Блок сообщений сервера [SMB] связанные плагины и плагин #10859) — обоснование позади этого подхода состоит в том, что достаточно достаточно обнаружить, является ли машиной, которая подразумевает быть хостом Linux, хостом Mac или любой другой отличной от Windows система, фактически Система Windows. Самый легкий способ сделать это должно включить некоторые связанные с SMB подключения Nessus, в частности сменный id# 10859 (SMB получают SID хоста). Этот плагин должен только возвращаемые значения для Систем Windows. Следовательно, если это возвращает информацию, можно безопасно прийти к заключению, что система выполняет операционную систему Windows. Можно также использовать плагины, которые восстанавливают информацию с Систем Windows тот NetBIOS использования. Если система возвратит сведения NetBIOS, то это, вероятно, будет Система Windows.**Внимание. :** Могли бы быть ошибочные допуски, такие как машины Linux, которые выполняют Samba.

Выполните эти шаги для настройки Менеджера Cisco Clean Access для выполнения сетевого просмотра с помощью подключений Nessus:

1. Откройте Менеджера Cisco Clean Access веб - консоль в браузере и входе в систему как администратор.
2. Выберите **Clean Access> Network Scanner** для доступа к Странице настройки Просмотра.
3. С набором Роли к роли пользователя вы хотите просмотреть, и набор операционной системы ко **Всем**, выбрать плагин, упомянутый в Плагинах для Получения информации из элемента с буллитами Систем Windows в этом документе (например, #10859).
4. Установите 'Уязвимый, Если …', устанавливающие в **ДЫРУ, ПРЕДУПРЕДИТЕ, ИНФОРМАЦИЯ** в разделе Уязвимостей.
5. Отключите просмотр для операционных систем Windows:Выберите **WIN_ALL** от выпадающего списка операционной системы.Отключите просмотр для этого выбора.

Сводка

Этот документ предоставляет механизм для использования Сети Cisco Clean Access Сканирование функции для обнаружения пользователей, которые симулируют использовать отличную от Windows система. Обратите внимание на то, что могло бы быть несколько других плагинов, доступных, который может сделать лучшее задание при обнаружении операционных систем. Как пример, с помощью nmap программного средства сканирования сети, xprobe2 от Системной безопасности, и т.д мог бы соответствовать потребностям лучше. Также обратите внимание, что сетевое сканирование не могло бы быть в состоянии предоставить надежные результаты, если клиентский компьютер выполняет персональный межсетевой экран.

Примечания

- Nessus является зарегистрированной торговой маркой Надежной Сетевой безопасности.

- Необходимо зарегистрироваться в Надежной Безопасности для получения подключений Nessus.
- Когда вы модифицируете/создаете плагины, гарантируете, что вы совместимы с лицензированием и требованиями товарного знака для Nessus и Надежной Сетевой безопасностью.

Дополнительные сведения

- Cisco Clean Access (NAC-устройство) поддержка продуктов
- Cisco Systems – техническая поддержка и документация