Совместная работа EAP-TLS и сканера WinRS

В рамках данной лабораторной работы мы разберем что такое сканер, как он работает, какие бывают типы сканеров, способы аутентификации и покажем, какие проверки могут быть выполнены с помощью сканера. Также мы объясним процесс настройки сканера и клиента и разберем самые часто встречающиеся проблемы. Длительность выполнения лабораторной работы — 2 часа.

Сетевые сканеры безопасности

Уровень защищенности компьютерных систем от угроз безопасности зависит от многих факторов. При этом одним из определяющих факторов является адекватность конфигурации системного и прикладного программного обеспечения (ПО), средств защиты информации и активного сетевого оборудования существующим рискам. Перечисленные компоненты информационной системы (ИС) имеют сотни параметров, значения которых влияют на защищенность системы, что делает их анализ трудновыполнимой задачей.

Поэтому в современных ИС для анализа конфигурационных параметров системного и прикладного ПО, технических средств и средств защиты информации обычно используются специализированные программные средства — сканеры безопасности. Современные сканеры безопасности можно условно классифицировать по многим параметрам: по архитектуре, исходному коду, реализации, предназначению и т.д.

В данной лабораторной работе рассматривается работа механизма сканирования WinRS, который является встроенным протоколом в ОС Windows и является транспортом безагентского сканера AxelNAC. Интеграция данного протокола с AxelNAC позволяет проверять соответствие клиентского устройства политикам информационной безопасности (ИБ). В случаях, когда клиентское устройство не соответствует установленным политикам, оно будет изолироваться с ограничением доступа к сети для устранения несоответствий.

В данный момент поддерживается только метод аутентификации Basic, который предусматривает механизм аутентификации при помощи учетных данных. Для того чтобы сканер мог работать с клиентским устройством, необходимо настроить на нем WinRS.

Несмотря на то, что использование данного сканера подразумевает настройку службы на клиентском устройстве, он все равно считается безагентским, т.к. служба WinRS является предустановленной для каждого устройства на ОС Windows.

Принцип работы сканера безопасности

В AxelNAC применяется сканер соответствия (Compliance Scanner). Данные сканеры отвечают за выявление проблем, связанных с несоответствием политикам информационной безопасности в сети.

Данный сканер работает по следующему алгоритму:

1. Идентификация статуса антивирусного ПО и проверка актуальности баз;
2. Проверка наличия обязательных обновлений безопасности;
3. Проверка запущенных служб (например, DLP);
4. Вызов события безопасности (например, изолирование устройства с последующим повторным сканированием).

Сканирование может проводиться в разное время, поэтому их принцип работы может быть разделен на три основных типа:

- **Сканирование до регистрации** — в таком случае сканер будет производить проверку до того как зарегистрировать клиентское устройство в сети. Такой способ является самым ненадежным, потому что до регистрации сканер не имеет полного доступа и может быть обманут при помощи вредоносного ПО;
- **Сканирование при регистрации** — при таком типе сканирования проверка будет производиться во время регистрации клиентского устройства. Сканирование начнется после перехода пользователем на Captive-портал AxelNAC, что гарантирует сетевую связность со сканируемым АРМ. Мы рекомендуем использовать данный тип совместно со сканированием после регистрации, чтобы периодически проверять клиентское устройство в процессе его работы в сети;
- **Сканирование после регистрации** — в таком случае сканер будет производить периодическую проверку клиентского устройства после его регистрации в сети.

Выполнение проверок с помощью сканера безопасности

На текущий момент с помощью сканера WinRS в AxelNAC можно проверять подключаемые клиентские устройства на соответствие следующим параметрам:

- **Обновление ОС** — данный параметр позволяет включить проверку наличия обновлений ОС. Также вы можете указать конкретное количество дней с момента последнего обновления (значение по умолчанию — 30 дней);
- **Требуемые пакеты обновлений ОС** — данный параметр позволяет включить проверку наличия конкретных пакетов обновлений ОС. В поле ниже необходимо указать все требуемые пакеты обновлений через пробел;
- **Проверка антивируса** — данный параметр позволяет включить проверку наличия включенного антивируса. В данный момент поддержана проверка **Kaspersky Endpoint Security** и **Windows Defender**;
- **Величина обновления баз антивируса** — данный параметр позволяет включить проверку наличия обновлений баз антивируса. Также вы можете указать конкретное количество дней с момента последнего обновления (значение по умолчанию — 14 дней);
- **Запущенные службы** — данный параметр позволяет включить проверку наличия запущенных служб Windows. В поле ниже необходимо указать все требуемые службы через пробел;
- **Проверка автозагрузки служб** — данный параметр позволяет проверить, включена ли автозагрузка перечисленных служб.

После проведения проверки, формируется отчет, значения (триггеры) из которого могут быть использованы в событиях безопасности. В таблице ниже приведены все возможные значения.

Таблица 1 — Список триггеров и условий их срабатывания во время сканирования

Наименование триггера	Условие срабатывания
ScanIsFailed	Не удалось подключиться к клиентскому устройству через сканер WinRS
ScanIsSuccess	Удалось подключиться к клиентскому устройству через сканер WinRS (при этом неважно было ли проведено сканирование дальше)
OsIsNotUpdated	Срабатывание при выполнении хотя бы одного из условия: • Последний поиск обновлений был выполнен больше значения поля **"Допустимое количество дней с момента последнего обновления"** • В списке обновлений на установку есть хотя бы одно обновление типа**"Critical Updates"** или **"Security Update"**
OsKBPatchesAreNotInstalled	Среди списка обновлений на установку есть хотя бы одно из значений**"Обновления требуемые для проверки"**
AntivirusIsNotInstalled	Не удалось найти установленный антивирус
AntivirusDefenderIsNotInstalled	Не установлен антивирус **Windows Defender**
AntivirusKESIsNotInstalled	Не установлен антивирус **Kaspersky Endpoint Security**

Наименование триггера	Условие срабатывания
AntivirusIsNotTurnedOn	Нет ни одного запущенного антивируса
AntivirusDefenderIsNotTurnedOn	Антивирус **Windows Defender** не запущен
AntivirusKESIsNotTurnedOn	Антивирус **Kaspersky Endpoint Security** не запущен
AntivirusIsNotUpdated	Антивирус не содержит обновленные антивирусные базы
AntivirusDefenderIsNotUpdated	Срабатывание при выполнении хотя бы одного из условий: • Статус антивируса **Windows Defender** — "не обновлен" • Дата последнего успешного поиска обновлений больше значения **"Допустимый порог устаревания антивирусных баз"**
AntivirusKESIsNotUpdated	Срабатывание при выполнении хотя бы одного из условий: • Статус антивируса **Kaspersky Endpoint Security** — "не обновлен" • Дата последнего успешного поиска обновлений больше значения **"Допустимый порог устаревания антивирусных баз"**

Настройка сканера безопасности в AxelNAC

Для того чтобы настроить работу сканера безопасности в AxelNAC, необходимо выполнить следующие этапы:

- Настройка коммутатора для работы CoA;
- Создание механизма сканирования;
- Создание события безопасности;
- Добавление механизма сканирования в профиль подключения.

Настройка коммутатора для работы с возможности изоляции пользователей

Для того чтобы коммутатор мог изолировать пользователей при несоблюдении политик безопасности, необходимо настроить службу Web-redirect.

Шаг 1. Перейдите в раздел **Конфигурация → Политика и контроль доступа → Сетевые устройства → Сетевые устройства** и выберите коммутатор, который вы создали в рамках лабораторной работы №1.

Шаг 2. На вкладке **Определение** активируйте параметр **Обеспечение работы внешнего портала**.

Шаг 3. На вкладке **Роли** перейдите в блок **Назначение VLAN ID** и в строке **isolation** укажите идентификатор VLAN, в которую будет изолироваться пользователь.

Шаг 4. В блоке **Назначение URL веб-аутентификации** в строке **isolate** укажите следующие данные: **http(s)://адрес_AxelNAC/Cisco::Catalyst_2960/** и нажмите **Сохранить**.

Шаг 5. В блоке **Назначение Local ACL** активируйте параметр **Назначать Local ACL** и в строке **isolation** укажите название ACL — **isolate** (данный ACL позже будет создан на коммутаторе).

Шаг 6. Подключитесь к коммутатору по протоколу SSH как администратор.

Шаг 7. Включите механизм Change-of-Authorization (CoA) с помощью следующих команд:

```
aaa server radius dynamic-author
client 172.20.100.2 server-key useStrongerSecret
port 3799
```

Шаг 8. Включите веб-аутентификацию с помощью следующих команд:

```
ip device tracking
ip http server
ip http secure-server
```

Шаг 9. Добавьте ACL с именем **isolate** с помощью следующих команд:

```
ip access-list extended isolate
deny ip any host 172.20.100.2
permit tcp any any eq www
permit tcp any any eq 443
```

Для корректной работы сканера необходимо указать ip helper в сторону AxelNAC.

Создание механизма сканирования

Создание механизма сканирования производится следующим образом:

Шаг 1. Перейдите в раздел **Конфигурация → Соответствие → Механизмы сканирования** и нажмите кнопку **Новый механизм сканирования**. В выпадающем списке выберите значение **WinRS**.

Шаг 2. Введите имя механизма сканирования в поле **Имя** и выберите значение **Basic authentication** в поле **Метод аутентификации**.

Шаг 3. Введите имя пользователя и пароль учетной записи клиентского устройства.

Шаг 4. Активируйте следующие переключатели:

- **Обновление ОС**;
- **Проверка антивируса**;
- **Запущенные службы → cAmSVc**;
- **Сканировать после регистрации**.

Шаг 5. Отключите параметр **Сканировать при регистрации**.

Шаг 6. Нажмите **Создать**.

Запомните имя созданного механизма, оно понадобится для следующих этапов лабораторной работы.

Создание события безопасности

Для создания события безопасности необходимо выполнить следующие шаги:

Шаг 1. Перейдите в раздел **Конфигурация → Соответствие → События в системе безопасности** и нажмите **Новое событие в системе безопасности**.

Шаг 2. В окне **Новое событие безопасности** включите срабатывание и внесите описание события безопасности.

Шаг 3. Нажмите **Добавить триггер**, в колонке **Событие** выберите значение **WinRS**, затем введите триггер **AntivirusKESIsNotInstalled**.

Шаг 4. Нажмите на иконку **+** и в колонке **Событие** снова выберите значение **WinRS**, затем введите триггер **AntivirusKESIsNotUpdated**.

Шаг 5. В строке **Действия, связанные с событием** активируйте переключатель **Изолировать** и заполните окно настроек следующим образом:

- **Роль во время изоляции** — Isolate;
- **Шаблон для использования** — failed_scan.html;
- **Текст кнопки** — Просканировать повторно;
- **Активировать автоматически** — Да;
- **Максимальное число попыток** — 99.

Шаг 6. В строке **Grace** укажите значение **1 секунда** и нажмите **Создать**.

Добавление механизма сканирования в профиль подключения

После того как процесс и логика работы сканера настроены, необходимо добавить сканер в профиль подключения:

Шаг 1. Перейдите в раздел **Конфигурация → Политика и контроль доступа → Профили подключения** и откройте профиль подключения, который вы создали в рамках лабораторной работы №1.

Шаг 2. На странице **Стандартный профиль подключения** в строке **Сканеры** нажмите на кнопку **Добавить сканер** и укажите имя сканера, созданного в рамках этой лабораторной работы, затем нажмите **Сохранить**.

Настройка Captive-портал

Для того чтобы сканирование проводилось, необходимо также настроить Captive-портал на сервере:

Шаг 1. Перейдите в раздел **Конфигурация → Сетевое взаимодействие → Интерфейсы** и выберите интерфейс, на котором необходимо включить функционал Captive-портала.

Шаг 2. В строке **Дополнительный демон (демоны) прослушивания** добавьте значение **портал** из выпадающего списка, затем нажмите **Сохранить**.

Шаг 3. Перейдите в раздел **Статус → Службы** и перезапустите следующие службы:

- haproxy-portal;
- httpd.portal;
- iptables.

Настройка клиентского устройства для работы со сканером безопасности

Для того чтобы сканер имел доступ к клиентскому устройству, на нем необходимо настроить службу WinRM. Чтобы произвести настройку, выполните следующие команды в Windows PowerShell от имени администратора:

```
winrm quickconfig                // данная команда запускает режим быстрой конфигурации службы WinRM
cd WSman:\localhost\
cd Client
set-item AllowUnencrypted $true  // данная команда разрешает незащищенное подключение к устройству
set-item TrustedHosts "*"        // данная команда разрешает подключение всех клиентов к устройству (* может быть заменена на конкретный IP-адрес или доменное имя)
cd ..\Service
set-item AllowUnencrypted $true  // данная команда разрешает незащищенное подключение локально для службы
cd Auth
set-item Basic $true             // данная команда включает базовую аутентификацию глобально
```

Настройка данной службы может быть проверена с помощью команды winrm get winrm/config. В ответе должен содержаться следующий лог:

```
Config
    MaxEnvelopeSizekb = 500
    MaxTimeoutms = 60000
    MaxBatchItems = 32000
    MaxProviderRequests = 4294967295
    Client
        NetworkDelayms = 5000
        URLPrefix = wsman
        AllowUnencrypted = true
        Auth
            Basic = true
            Digest = true
            Kerberos = true
            Negotiate = true
            Certificate = true
            CredSSP = false
        DefaultPorts
            HTTP = 5985
            HTTPS = 5986
        TrustedHosts = *
    Service
        RootSDDL = O:nsg:BAD:P(A;;GA;;;BA)(A;;GR;;;IU)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW;;;WD)
        MaxConcurrentOperations = 4294967295
        MaxConcurrentOperationsPerUser = 1500
        EnumerationTimeoutms = 240000
        MaxConnections = 300
        MaxPacketRetrievalTimeSeconds = 120
        AllowUnencrypted = true
        Auth
            Basic = true
            Kerberos = true
            Negotiate = true
            Certificate = false
            CredSSP = false
            CbtHardeningLevel = Relaxed
        DefaultPorts
            HTTP = 5985
            HTTPS = 5986
        IPv4Filter = *
        IPv6Filter = *
        EnableCompatibilityHttpListener = false
```

EnableCompatibilityHttpsListener = false
CertificateThumbprint
AllowRemoteAccess = true
Winrs
AllowRemoteShellAccess = true
IdleTimeout = 7200000
MaxConcurrentUsers = 2147483647
MaxShellRunTime = 2147483647
MaxProcessesPerShell = 2147483647
MaxMemoryPerShellMB = 2147483647
MaxShellsPerUser = 2147483647

Проверка работы механизма сканирования

После того как все настройки, необходимые для проведения сканирования, выполнены, проверьте его работу. Для этого подключите конечное устройство, на котором не установлен/не запущен антивирус Kaspersky Endpoint Security к сети. При правильной настройке на устройстве откроется страница с информацией о причине изоляции и кнопкой **Просканировать повторно**. На стороне AxelNAC в разделе **Отчеты → События безопасности → Открытые** вы увидите соответствующее событие безопасности в списке.

Затем установите/запустите антивирус Kaspersky Endpoint Security на конечном устройстве и нажмите **Просканировать повторно**. После этого устройство должно быть перемещено в общую сеть. На стороне AxelNAC событие безопасности перейдет в статус **Закрытое** и будет доступно в разделе **Отчеты → События безопасности → Закрытые**.

Решение самых часто встречающихся проблем

Событие безопасности "post reg system scan" было создано и не закрывается

Данная проблема может быть вызвана несколькими причинами:

- Проверьте доступен ли TCP-порт 5985 у сканируемого АРМ;
- Проверьте корректность логина и пароля в web-интерфейсе AxelNAC;
- Проверьте, что пользователь, указанный вами в web-интерфейсе AxelNAC, не содержит ".\";
- Проверьте права локального пользователя — пользователь должен обладать правами администратора.

Событие безопасности post reg system scan не было создано

Проверьте, что AxelNAC получает информацию об актуальном IP-адресе АРМ. Для этого перейдите в раздел **Узлы** и укажите MAC-адрес клиента в строке поиска. После этого перейдите в профиль устройства — на вкладке ipv4 будет находиться актуальный адрес клиента, полученный из **ip helper-address**. Если адреса нет, проверьте, указан ли адрес AxelNAC в ip helper на сетевом оборудовании.––

Если событие безопасности не создается, хотя AxelNAC знает актуальный адрес АРМ, перейдите на вкладу **Конфигурация → Соответствие → События безопасности** и откройте любое событие безопасности, после чего нажмите **Сохранить**.

ID статьи: 10
Последнее обновление: 2 дек., 2025
Обновлено от: Ильина В.
Ревизия: 23
База знаний AxelNAC -> Обучающие материалы -> Лабораторные работы -> Совместная работа EAP-TLS и сканера WinRS
https://docs.axel.pro/entry/10/