Совместная работа EAP-TLS и механизма сканирования AxelNAC

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 наиболее 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 AxelNAC, который позволяет проводить проверку соответствия заданным политикам безопасности. Он проверяет устройства на базе Windows с помощью протокола подключения к сканируемому устройству WinRS и Linux с помощью протокола подключения к сканируемому устройству SSH. Конфигурация сканера может включать в себя как WinRS или SSH, так и оба протокола одновременно. AxelNAC выберет подходящий под ОС устройства протокол.

Протокол WinRS

Протокол WinRS использует службу **winrm**, которая является встроенной по умолчанию в ОС Windows и выступает в роли транспорта безагентского сканера **AxelNAC**.

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

Протокол SSH

Протокол SSH использует службу **ssh**, которая по умолчанию встроена в большинство дистрибутивов Linux. При подключении к клиентскому устройству сканеру необходимо пройти процесс аутентификации. Аутентификация производится с использованием сертификата клиента. Он должен быть подписан Центром сертификатов AxelNAC, который создан на вкладке **SSH Аутентификация на основе сертификата** .

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 данный момент для устройств на базе **ОС Windows** существуют следующие параметры для настройки политик безопасности:

- Обновление ОС;
- Проверка антивируса;
- Проверка обновлений баз антивируса;
- Принадлежность пользователя к домену;
- Дополнительная проверка имени пользователя;
- Проверка обновлений безопасности ОС;
- Запущенные службы;
- Проверка автозапуска служб.

Для устройств на базе **Unix-систем** существуют следующие параметры для настройки политик безопасности:

- Проверка статуса антивируса;
- Проверка версии антивируса;
- Проверка обновлений антивируса;
- Обновление ядра ОС;
- Принадлежность к группам;
- Запущенные службы;
- Проверка автозапуска служб;
- Проверка файлов;
- Список файлов;
- Проверка хэш-суммы.

После проведения проверки, формируется отчет, значения (триггеры) из которого могут быть использованы в событиях безопасности. Все возможные значения вы можете увидеть в данной статье.

Настройка сканера безопасности в AxelNAC

Механизм сканирования AxelNAC позволяет выполнять сканирование с устройствами на базе как Unix-систем, так и Windows. Для того чтобы настроить работу сканера безопасности в AxelNAC, необходимо выполнить следующие этапы:

- Настройка коммутатора для работы с возможностью изоляции пользователей.
- Создание центра сертификации для работы протокола SSH.
- Создание механизма сканирования.

- Добавление механизма сканирования в профиль подключения.
- Создание события безопасности.

Настройка коммутатора для работы с возможностью 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.

Настройка механизма сканирования по протоколу SSH

Создание центра сертификации для работы протокола SSH

Шаг 1. Перейдите в раздел **Конфигурация → Соответствие → Механизмы сканирования → SSH Аутентификация на основе сертификата** и нажмите **Новый SSH Центр аутентификации на основе сертификата**.

Шаг 2. В открывшемся окне заполните поле **Имя** и нажмите **Сохранить**.

После этого страница обновится и вы увидите поле **Открытый ключ**, содержащее в себе значение созданного открытого ключа.

Удаление УЦ невозможно, если он используется в настройках сканера. Чтобы выполнить удаление, сначала исключите УЦ из конфигурации сканера или удалите сам сканер.

Во время создания УЦ генерируются закрытый и открытый ключи по следующим правилам:
• тип ключа — RSA;
• длина ключа — 4096 бит.
Данные правила невозможно изменить.

Создание механизма сканирования для работы протокола SSH

Для сканирования устройств на базе Unix-систем необходимо настроить протокол SSH, создав механизм сканирования. Создание производится следующим образом:

Шаг 1. В разделе **Конфигурация → Соответствие → Сканеры** нажмите **Новый механизм сканирования** и выберите **AxelNAC** в выпадающем списке.

Шаг 2. На открывшейся вкладке **Основные настройки** введите имя пользователя и пароль учетной записи клиентского устройства.

Шаг 3. Активируйте параметр **Сканировать после регистрации**.

Шаг 4. Отключите параметр **Сканировать при регистрации**.

Если ранее вы уже настроили протокол WinRS, выполнение шагов 1-4 не требуется.

Шаг 5. Перейдите на вкладку **SSH**.

Шаг 6. Заполните следующие параметры:

- **Включить SSH**: Включено.
- **Порт**: 22.
- **SSH Центр сертификатов для аутентификации пользователя** : Созданный ранее Центр сертификации.
- **Проверка статуса антивируса**: Включено.
- **Проверка версии антивируса**: Включено.
- **Проверка обновлений антивируса**: Включено.
- **Обновления ядра ОС**: Включено.

Шаг 7. Нажмите **Создать**.

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

Создание события безопасности для протокола SSH

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. На вкладке **Новое событие безопасности** активируйте параметр **Активировать событие безопасности** и внесите описание события безопасности.

Шаг 3. Добавьте триггеры для протокола SSH. Нажмите **Добавить триггер,** в колонке **Событие** снова выберите значение **AxelNAC**, затем введите триггер **KInagentNotRunning**.

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

Шаг 5. Нажмите на иконку **+** и в колонке **Событие** снова выберите значение **AxelNAC**, затем введите триггер **KESDatabaseOutOfDate**.

Шаг 6. Нажмите на иконку **+** и в колонке **Событие** снова выберите значение **AxelNAC**, затем введите триггер **KernelOutOfDate**.

Шаг 7. Нажмите на иконку **+** и в колонке **Событие** снова выберите значение **AxelNAC**, затем введите триггер **ReleaseOutOfDate**.

Шаг 8. Нажмите на иконку **+** и в колонке **Событие** снова выберите значение **AxelNAC**, затем введите триггер **PatchOutOfDate**.

Шаг 9. 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**: Включено;
- **Максимальное число попыток**: 99.

Шаг 10. В строке **Грейс-период** укажите значение **1 секунда** и нажмите **Создать**.

Настройка механизма сканирования по протоколу WinRS

Создание механизма сканирования для работы протокола WinRS

Для сканирования устройств на базе Windows необходимо настроить протокол WinRS, создав механизм сканирования. Создание производится следующим образом:

Шаг 1. В разделе **Конфигурация → Соответствие → Сканеры** нажмите **Новый механизм сканирования** и выберите **AxelNAC** в выпадающем списке.

Шаг 2. На открывшейся вкладке **Основные настройки** введите имя пользователя и пароль учетной записи клиентского устройства.

Шаг 3. Активируйте параметр **Сканировать после регистрации**.

Шаг 4. Отключите параметр **Сканировать при регистрации**.

Шаг 5. Перейдите на вкладку **WinRS**.

Шаг 6. Заполните следующие параметры:

- **Включить WinRS**: Включено.
- **Порт**: 5985.
- **Метод аутентификации**: Базовый.
- **Обновление ОС**: Включено.
- **Проверка антивируса**: Включено.
- **Запущенные службы**: cAmSVc.

Шаг 7. Нажмите **Создать**.

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

Создание события безопасности для протокола WinRS

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. На вкладке **Новое событие безопасности** активируйте параметр **Активировать событие безопасности** и внесите описание события безопасности.

Шаг 3. Добавьте триггеры для протокола WinRS. Нажмите **Добавить триггер**, в колонке **Событие** выберите значение **AxelNAC**, затем введите триггер **AntivirusKESIsNotInstalled**.

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

Шаг 5. Нажмите на иконку **+** и в колонке **Событие** снова выберите значение **AxelNAC**, затем введите триггер **OsIsNotUpdated**.

Шаг 6. Нажмите на иконку **+** и в колонке **Событие** снова выберите значение **AxelNAC**, затем введите триггер **ServiceIsNotRunning**.

Шаг 7. 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**: Включено;
- **Максимальное число попыток**: 99.

Шаг 8. В строке **Грейс-период** 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-портала

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 с протоколом WinRS

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 файл журнала:

```
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
```

Настройка клиентского устройства для работы с протоколом SSH

Для того чтобы сканер имел доступ к клиентскому устройству, на нем необходимо выполнить следующие настройки:

Шаг 1. В разделе **Конфигурация → Соответствие → Сканеры** выберите ранее созданный механизм сканирования.

Шаг 2. На вкладке **SSH** появится параметр **Установочный скрипт**. Нажмите **Скачать**, чтобы загрузить установочный скрипт, и проверьте, соответствует ли он требованиям вашей инфраструктуры. При необходимости внесите в скрипт изменения и запустите его на суппликанте.

Данный скрипт выполняет настройки **Учетной записи** с именем, указанным в параметре **Имя пользователя**, SSH-сервера и проверяет необходимые утилиты для проведения проверок. В настройках SSH-сервера скрипт устанавливает параметр **PubkeyAuthentication** в значение YES. Также он содержит параметр **TrustedUserCAKeys** с файлом открытого ключа удостоверяющего центра, указанного в параметре **SSH Центр сертификатов для аутентификации пользователя**.

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 наиболее 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 веб-интерфейсе AxelNAC;
- Проверьте, что пользователь, указанный вами в веб-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 вкладку **Конфигурация → Соответствие → События безопасности** и откройте любое событие безопасности, после чего нажмите **Сохранить**.

Активация работы Captive-портала на АРМ под управлением Unix-систем

В Unix-системах Captive-портал не открывается самостоятельно в браузере, поэтому используется скрипт, который отслеживает трафик и принудительно запускает Captive-портал в браузере. Приведенный по ссылке скрипт является примером и может быть использован как основа для собственной реализации.

ID статьи: 1477
Последнее обновление: 9 апр., 2026
Обновлено от: Егоров В.
Ревизия: 21
База знаний AxelNAC -> Обучающие материалы -> Лабораторные работы -> Совместная работа EAP-TLS и механизма сканирования AxelNAC
https://docs.axel.pro/entry/1477/