**Домашнее задание**

|  |  |
| --- | --- |
| Дисциплина | «Защита компьютерных сетей и систем» |
| Тема | Тема 29. «Системы обнаружения и предотвращения вторжений» |
| Форма проверки | **Автоматическая проверка** |
| Имя преподавателя | Антон Носков |
| Время выполнения | 60 минут |
| Цель задания | Научиться:   * включать IOS IPS, * настраивать ведение журнала, * изменять сигнатуры IPS, * осуществлять проверку IPS. |
| Инструменты для выполнения ДЗ | Компьютер, симулятор сети передачи данных Cisco Packet Tracer 8.1.1, подключенный к интернету. |
| Правила приёма работы | * Чтобы выполнить задание, используйте Cisco Packet Tracer. * Выполнив задание, нажмите Check Results («Проверить результаты»), чтобы просмотреть отзыв и проверить завершённые обязательные компоненты. * Файл с выполненным заданием сохраните под своей фамилией и разместите в ЛМС **(ФИО.pka).** В отдельном файле прикрепите ответы на вопросы из второй части задания. |
| Критерии оценки | **Задание считается выполненным, если:**  - Check Results выдаёт положительный отзыв и все обязательные компоненты выполнены;  - ссылка на файл с сохранённым заданием размещена в ЛМС.  **Задание не выполнено, если:**  - Check Results выдаёт ошибки — нужно проработать ошибки и выполнить Check Results ещё раз;  - ссылка на файл с заданием не размещена в ЛМС. |
| Дедлайн | *две недели после вебинара (точную дату см. в ЛМС).* |

**Описание задания**

**Прежде чем выполнять задание, установите симулятор сети передачи данных Cisco Packet Tracer 8.1.1.**

<https://disk.yandex.ru/d/SdBaqlDc012UYA> — Cisco Packet Tracer 8.1.1 — Windows 64.

<https://disk.yandex.ru/d/dU9AL1YstQzFGg> — Cisco Packet Tracer 8.1.1 — Ubuntu 64.

<https://disk.yandex.ru/d/jwvB6MfZyPZ5sw> — Cisco Packet tracer 8.1.1 — MacOS X.

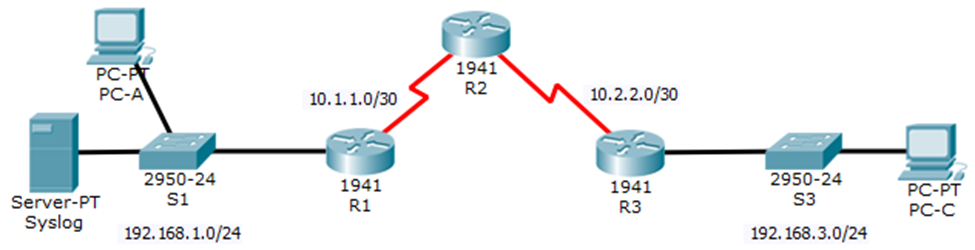
*Инструкция по установке*

Когда Cisco Packet Tracer выдаёт запрос авторизации, выберите Skills for all и авторизуйтесь через учётную запись Google. В ряде сетей может потребоваться VPN при запуске Cisco Packet Tracer.

После установки Cisco Packet Tracer откройте файл **ISP.pka***(размещён в ЛМС)* и начинайте выполнять задание.

**Исходные данные**

**Топология сети**



**Таблица адресации**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Шлюз по умолчанию** | **Порт коммутатора** |
| R1 | G0/1 | 192.168.1.1 | 255.255.255.0 | Н/П | S1 F0/1 |
| S0/0/0 | 10.1.1.1 | 255.255.255.252 | Н/П | Н/П |
| R2 | S0/0/0 (DCE) | 10.1.1.2 | 255.255.255.252 | Н/П | Н/П |
| S0/0/1 (DCE) | 10.2.2.2 | 255.255.255.252 | Н/П | Н/П |
| R3 | G0/1 | 192.168.3.1 | 255.255.255.0 | Н/П | S3 F0/1 |
| S0/0/0 | 10.2.2.1 | 255.255.255.252 | Н/П | Н/П |
| Syslog | NIC | 192.168.1.50 | 255.255.255.0 | 192.168.1.1 | S1 F0/2 |
| PC-A | NIC | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 | S1 F0/3 |
| PC-C | NIC | 192.168.3.2 | 255.255.255.0 | 192.168.3.1 | S3 F0/2 |

**Исходный сценарий**

Ваша задача — включить систему IPS на маршрутизаторе R1 для проверки трафика, поступающего в сеть 192.168.1.0.

Сервер Syslog используется для ведения журнала сообщений IPS. Вы должны настроить маршрутизатор для идентификации сервера Syslog, который будет получать сообщения журнала. При использовании сервиса для мониторинга сети очень важно, чтобы в сообщениях syslog отображались правильные дата и время. Настройте часы и сервис временных меток для ведения журналов на маршрутизаторах. Включите систему IPS для выдачи оповещения и отбрасывания пакетов ICMP Echo Reply во внутриканальном режиме.

Сервер и компьютеры были предварительно настроены. На маршрутизаторах также были предварительно настроены следующие параметры:

* пароль привилегированного доступа: **ciscoenpa55;**
* пароль консоли: **ciscoconpa55;**
* имя пользователя и пароль SSH: **SSHadmin/ciscosshpa55;**
* OSPF 101.

**Часть 1. Включение IOS IPS**

**Примечание:** в Packet Tracer файлы сигнатур уже импортированы на маршрутизаторы. Это XML-файлы по умолчанию, хранящиеся во флеш-памяти. По этой причине не нужно настраивать открытый криптографический ключ и вручную импортировать файлы сигнатур.

**Шаг 1. Включение пакета Security Technology:**

a. на маршрутизаторе **R1** введите команду **show version** для просмотра сведений о лицензии Technology Package;

b. если пакет Security Technology не активирован, сделайте это с помощью следующей команды:

R1(config)# **license boot module c1900 technology-package securityk9**

c. примите условия лицензионного соглашения с конечным пользователем;

d. сохраните текущую конфигурацию и перезагрузите маршрутизатор, чтобы включить лицензию;

e. убедитесь, что пакет Security Technology включён, с помощью команды **show version**.

**Шаг 2. Проверка связи по сети:**

a. отправьте эхо-запрос с компьютера **PC-C** на компьютер **PC-A**. Эхо-запрос должен быть выполнен успешно;

b. отправьте эхо-запрос с компьютера **PC-A** на компьютер **PC-C**. Эхо-запрос должен быть выполнен успешно.

**Шаг 3. Создание каталога конфигурации IOS IPS во флеш-памяти.**

На маршрутизаторе **R1** создайте каталог во флеш-памяти c помощью команды **mkdir.** Присвойте каталогу имя **ipsdir**.

**Шаг 4. Настройка каталога для хранения сигнатур IPS.**

На маршрутизаторе **R1** задайте только что созданный каталог в качестве места хранения сигнатур IPS.

**Шаг 5. Создание правила IPS.**

На маршрутизаторе **R1** создайте имя правила IPS c помощью команды **ip** **ips name** *name* в режиме глобальной настройки. Присвойте правилу IPS имя **iosips**.

**Шаг 6. Включение ведения журнала.**

Система IPS в iOS поддерживает использование Syslog для отправки уведомлений о событиях. Функция уведомлений Syslog включена по умолчанию. Если консоль ведения журналов включена, будут отображаться сообщения Syslog, касающиеся IPS:

a. если сервис Syslog не включён, включите его;

b. при необходимости сбросьте часы c помощью команды **clock set** в привилегированном режиме;

c. убедитесь, что на маршрутизаторе включён сервис временных меток для ведения журналов, c помощью команды **show run**. Если сервис временных меток не включён, включите его;

d. отправьте журнальные сообщения на сервер Syslog по IP-адресу 192.168.1.50.

**Шаг 7. Настройка системы IPS в iOS на использование категорий сигнатур.**

Выведите из использования категорию сигнатур **all** c помощью команды **retired true** (все сигнатуры в выпуске сигнатур). Верните в использование категорию **IOS\_IPS Basic** c помощью команды **retired false**.

**Шаг 8. Применение к интерфейсу правила IPS.**

Примените к интерфейсу правило IPS c помощью команды **ip** **ips name** *direction* в режиме настройки интерфейса. Примените правило для исходящего трафика (outbound) на интерфейсе G0/1 маршрутизатора R1. После включения IPS некоторые журнальные сообщения будут отправлены на линию консоли, указывая на выполнение инициализации механизмов IPS.

**Примечание.** Направление **in** означает, что система IPS проверяет только трафик, входящий на интерфейс. Аналогичным образом направление **out** означает, что система IPS проверяет только трафик, исходящий из интерфейса.

**Часть 2. Изменение сигнатуры**

**Шаг 1. Изменение для сигнатуры действия при наступлении события (параметр event-action).**

Верните в использование сигнатуру эхо-запроса (сигнатура 2004, идентификатор subsig 0), включите её и измените действие сигнатуры на оповещение и отбрасывание.

**Шаг 2. Проверка IPS c помощью команд show.**

Используйте команду **show ip ips all** для просмотра сводки состояний конфигураций IPS.

К каким интерфейсам и в каком направлении применяется правило **iosips**?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Шаг 3. Проверка правильности работы IPS:**

a. попробуйте отправить эхо-запрос с компьютера **PC-C** на **PC-A**. Эхо-запрос выполнен успешно? Поясните ответ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

b. попробуйте отправить эхо-запрос с компьютера **PC-A** на **PC-C**. Эхо-запрос выполнен успешно? Поясните ответ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Шаг 4. Просмотр сообщений Syslog:**

a. выберите сервер **Syslog**,

b. перейдите на вкладку **Services**,

c. в левом меню навигации выберите **SYSLOG** для просмотра файла журнала.

**Проверка результатов**

Вы полностью выполнили задание. Нажмите **Check Results («Проверить результаты»)** для просмотра отзыва и проверки завершённых обязательных компонентов.