Lab: Конфигурация и защита Сетевых устройств с использованием SSH

Топология и таблица адресации

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Цели лабораторной работы

- Настроить базовые параметры устройств.
- Настроить SSH-доступ на маршрутизаторе и коммутаторе.
- Применить меры безопасности согласно лучшим практикам.
- Проверить работу SSH и корректность настроек безопасности.

Часть 1: Настройка базовых параметров устройств

1. Подключите устройства согласно топологии.
2. Инициализируйте и перезагрузите маршрутизатор и коммутатор.
3. Настройте базовые параметры:
    a. Название устройства.
    b. Отключение DNS lookup.
    c. Привилегированный пароль: `class` (зашифрован).
    d. Консольный пароль: `cisco`, вход включен.
    e. Пароль VTY: `cisco`, вход включен.
    f. Баннер предупреждения о несанкционированном доступе.
    g. IP-адреса интерфейсов (G0/0/1 и VLAN 1).
    h. Сохраните конфигурации.

4. Настройте PC-A с IP, маской и шлюзом.
5. Проверьте доступность устройств через `ping`.

Часть 2: Настройка SSH-доступа и безопасности на маршрутизаторе (R1)

1. Установите имя устройства и домен
2. Создайте пользователя `SSHadmin` с паролем `55HAdm!n2025`
3. Разрешите только SSH на VTY
4. Зашифруйте пароли
5. Измените пароли:
6. Убедитесь, что все неиспользуемые интерфейсы отключены.

Часть 3: Настройка SSH-доступа и безопасности на коммутаторе (S1)

Повторите аналогичные шаги:

1. Назначьте имя устройства и домен.
2. Создайте пользователя `SSHadmin` с паролем `55HAdm!n2020`.
3. Генерация ключей RSA 1024.
4. Разрешите только SSH на VTY.
5. Зашифруйте все пароли.
6. Установите длину пароля минимум 12 символов.
7. Измените пароли
8. Настройка тайм-аутов и блокировок входа.
9. Отключите все неиспользуемые порты

Часть 4: Проверка SSH и настроек безопасности

1. Подключитесь к R1 и S1 с ПК-A через SSH (используйте Tera Term).
2. Убедитесь, что Telnet запрещён.
3. Проверьте, что при ошибочных попытках входа доступ блокируется.
4. Просмотрите текущий статус и настройки.

Исследование угроз сетевой безопасности и защита устройств с помощью SSH

Цели

- Изучить авторитетные источники по угрозам сетевой безопасности.
- Выявить актуальные угрозы, связанные с удалённым управлением устройствами.
- Проанализировать одну из угроз более подробно.
- Соотнести угрозу с мерами защиты, реализуемыми на маршрутизаторе и коммутаторе.

Часть 5: Изучение ресурсов по безопасности

1. Перейдите на сайт SANS и найдите раздел **FREE Resources**.
2. Изучите доступные ресурсы.

Примеры полезных ресурсов:

- SANS Newsletters (в том числе @Risk).
- Critical Security Controls (например, SSH и безопасная авторизация).
- Security Awareness Posters.

3. Откройте **Critical Security Controls** и выберите контроль, связанный с **управлением доступом к устройствам** (например, Control 4: Controlled Use of Administrative Privileges).

Рекомендации по реализации:

- Использовать только зашифрованные протоколы доступа (например, SSH вместо Telnet).
- Применять многофакторную аутентификацию.
- Лимитировать число попыток входа.

Часть 6: Выявление современных угроз, связанных с SSH и авторизацией

1. Откройте архив @RISK Security Alerts.

2. Просмотрите последние выпуски, найдите угрозы, связанные с:
    a. Слабым шифрованием SSH.
    b. Атаками перебора паролей (brute force).
    c. Уязвимостями в реализации SSH на устройствах (например, CVE-2023-48788).

Пример уязвимости:

- *OpenSSH Remote Code Execution Vulnerability* — позволяет атакующему выполнить команды на устройстве через уязвимость в обработке SSH.

3. Дополнительные ресурсы:
    a. NIST National Vulnerability Database (nvd.nist.gov)
    b. CISA – Cybersecurity & Infrastructure Security Agency
    c. SecurityFocus

Недавние угрозы:

- CVE-2023-38408: Уязвимость в OpenSSH forwarding.
- Ботнеты, использующие стандартные логины через Telnet и SSH.

Часть 7: Исследование конкретной атаки

Заполните представленную ниже форму выбрав определенный тип атаки

Name of attack:	
Type of attack:	
Dates of attacks:	
Computers / Organizations affected:	
How it works and what it did:	
Mitigation options:	
References and info links:	