**ЗВІТ**

з виконання лабораторної роботи № 2

курсантом навчальної групи

.

**Тема:** Дослідження функцій захищеного віддаленого доступу та захисту мережевого обладнання *Cisco* від несанкціонованого використання

**Мета заняття**: дослідження принципів організації захищеного віддаленого доступу до мережевого обладнання *Cisco*, вивчення методів автентифікації користувачів та захисту пристроїв від несанкціонованого використання, а також набуття практичних навичок налаштування сервісів *Telnet, SSH* і механізмів *Port Security* з метою підвищення рівня безпеки локальної мережі.

**Очікувані результати заняття:**

1. Знати, вміти відтворити (вибрати) визначення та теоретичні відомості, що наведені в Л6 – Л8.

2. Налаштувати та продемонструвати функції захищеного віддаленого доступу до мережевого обладнання *Cisco* за протоколами *Telnet* і *SSH*.

3. Застосувати на практиці команди *Cisco IOS* для створення та перевірки віртуальних інтерфейсів (*SVI*) і встановити взаємозв’язок між *IP*-адресацією та віддаленим доступом.

4. Дослідити та пояснити принципи автентифікації користувачів і інтерпретувати різницю між шифрованим і нешифрованим з’єднанням.

5. Виконати налаштування засобів *Port Security* та оцінити ефективність їх застосування для запобігання несанкціонованому доступу.

6. Класифікувати та порівняти режими реагування *Port Security* (*Protect, Restrict, Shutdown*) і робити висновки щодо їх придатності у різних сценаріях.

7. Проілюструвати та узагальнити результати досліджень у вигляді скріншотів, таблиць і висновків у звіті.

8. Встановити взаємозв’язок між конфігураціями мережевих пристроїв і політиками безпеки організації.

9. Узагальнити отримані результати досліджень та оцінити ефективність побудованих локальних.

10. Вміти оформлювати звіт з лабораторної роботи

**1. Дослідження функції захищеного віддаленого доступу до мережевого обладнання *Cisco* за протоколом *Telnet*.**

*Завдання 1.1. Здійсніть розгортання навчальної локальної мережі на двох комутаторах Cisco 2960.*

5. Схема начальної мережі у звіті.

*Місце вставлення скріншоту*

6. Перехід до привілейованого режиму після здійснення початкових налаштувань

*Місце вставлення скріншоту*

7. Результат виконання команди ***ping***:

*Місце вставлення скріншоту*

6. Таблиця під’єднання пристроїв до комутаторів

|  |  |  |  |
| --- | --- | --- | --- |
| Ім’я комутатора | Інтерфейс комутатора до якого підключений пристрій | Ім’я пристрою який підключений до комутатора | Інтерфейс пристрою, через який здійснено підключення до комутатора |
| *Telnet\_Switch 0* |  |  |  |
| *Telnet\_Switch 0* |  |  |  |
| *SSH\_Switch 1* |  |  |  |
| *SSH\_Switch 1* |  |  |  |

*Завдання 1.2. Здійсніть налаштування віртуального інтерфейсу (SVI) комутатора на першому комутаторі.*

2. Команди для налаштування **віртуального інтерфейсу:**

*Місце вставлення команд*

3. Результат перевірки доступу до віртуального інтерфейсу:

*Місце вставлення скріншоту*

4. Відомості про *SVI* на комутаторі *Telnet:*

*Місце вставлення скріншоту*

*Завдання 1.3. Дослідіть функції захищеного віддаленого доступу до мережевого обладнання Cisco за протоколом Telnet.*

2. Команди для налаштування віддаленого доступу по протоколу *telnet:*

*Місце вставлення команд*

3. Інформація про налаштовані віртуальні лінії *vty* 0 4:

*Місце вставлення скріншоту*

Пароль зберігається в *Ваша відповідь* вигляді.

5. Результат з’єднання комутатором за протоколом *Telnet*:

*Місце вставлення скріншоту*

6. Результат спроби з’єднання з іншим комп’ютером:

*Місце вставлення скріншоту*

Даний результат може свідчити про *Ваша відповідь*

7. Результат спроби з’єднання з іншою *iP*-адресою, яка не зайнята жодним пристроєм

*Місце вставлення скріншоту*

Воно може свідчити про *Ваша відповідь*

**2. Забезпечення захищеної комунікації по протоколу SSH**

*Завдання 2.1 Налаштуйте віртуальний інтерфейс (SVI) на другому комутаторі.*

1. Перехід до привілейованого режиму після здійснення початкових налаштувань

*Місце вставлення скріншоту*

3. Результат перевірки доступу до віртуального інтерфейсу:

*Місце вставлення скріншоту*

4. Відомості про *SVI* на комутаторі *Telnet:*

*Місце вставлення скріншоту*

*Завдання 2.2* *Налаштуйте віддалений доступ по ssh до другого комутатора.*

2. Команди для налаштування віддаленого доступу по протоколу *ssh:*

*Місце вставлення команд*

3. Інформація про налаштовані віртуальні лінії *vty* 0 4:

*Місце вставлення скріншотів*

Пароль зберігається в *Ваша відповідь* вигляді.

5. Результат з’єднання комутатором за протоколом *SSH*:

*Місце вставлення скріншоту*

Після введення парою потрапляємо в *Ваша відповідь* режим.

6.Ім’я користувача *Ваша відповідь*

Пароль *Ваша відповідь*

7. Результат з’єднання комутатором за протоколом *SSH*:

*Місце вставлення скріншоту*

Після введення парою потрапляємо в *Ваша відповідь* режим.

На це вплинуло *Ваша відповідь*

**3. Дослідження функцій захисту мережевого обладнання від несанкціонованого використання**

*Завдання 3.1. Дослідіть функцію захисту комутатора за рахунок відключення портів, що не використовуються.*

5. При під’єднанні комп’ютера до вимкнених портів *Ваша відповідь*

Схема мережі з нелегальним комп’ютером:

*Місце вставлення скріншоту*

6. При під’єднанні нелегального комп’ютер до працюючого порту *Ваша відповідь*

7. Основний недолік функції захисту комутатора за рахунок відключення портів, що не використовуються полягає у тому, *Ваша відповідь*

*Завдання 3.2 Дослідіть функцію безпеки портів (функція Port Security).*

***Port-Security*** – це функція комутатора, за допомогою якої можна вказати яким пристроям дозволено передавати трафік через порти (інтерфейси) до яких вони під’єднані.

1. Команди для налаштування *функції Port Security:*

*Місце вставлення команд*

2. *МАС*-адреса легального комп’ютера: *Ваша відповідь*

3. Результат виконання команди *show port-security interface:*

*Місце вставлення скріншоту*

6. Відомості про нелегальний комп’ютер: *іР*-адреса: *Ваша відповідь*, *МАС*-адреса: *Ваша відповідь*

8. Результат перевірки здатності нелегального комп’ютера передавати інформацію:

*Місце вставлення скріншоту*

9. Результат перевірки здатності легального комп’ютера передавати інформацію:

*Місце вставлення скріншоту*

***Sticky*** *(*липкі*) MAC*-адреси

5. Результат виконання команди *show running-config*

*Місце вставлення скріншоту*

7. Результат виконання команди *show running-config:*

*Місце вставлення скріншоту*

Відбулись наступні зміни: *Ваша відповідь*

8. Таблиця 3.1. стан інтерфейсу та мережі при різних режимах реагування на порушення.

|  |  |  |  |
| --- | --- | --- | --- |
| Режим реагування при порушенні | Стан інтерфейсу | Чи здатні легальні пристрої передавати інформацію | Чи здатні нелегальні пристрої передавати інформацію |
| *Protect* | *Ваша відповідь* | *Ваша відповідь* | *Ваша відповідь* |
| *Restrict* | *Ваша відповідь* | *Ваша відповідь* | *Ваша відповідь* |
| *Shutdown* | *Ваша відповідь* | *Ваша відповідь* | *Ваша відповідь* |

**Висновок *Ваш загальний висновок* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |
| --- | --- |
| **Виконав:**  курсант навчальної групи  .  (в/звання, підпис ім’я та прізвище)  . 2025 | **Перевірив:**  професор кафедри КіТ та КБ  підполковник Володимир ОХРІМЧУК  (в/звання, підпис ім’я та прізвище)  . 2025 |
|  |  |