**Національний технічний університет України**

**«Київський політехнчний інститут імені Ігоря Сікорського»**

**Навчально-науковий інститут атомної та теплової енергетики**

**Кафедра цифрових технологій в енергетиці**

**Звіт**

**з лабораторної роботи №4**

**з дисципліни «Безпека інформаційних систем»**

Виконав:

студент групи ТР-23

Ровний Г.О.

КИЇВ - 2024

**Мета роботи:** лабораторна робота спрямована на набуття практичних навичок роботи в емуляторі Cisco Packet Tracer та дослідженні особливостей налаштування функціонування системи запобігання вторгненням IOS (IPS) за допомогою CLI.

**Поставлене завдання:**

1. Увімкнути IOS IPS.

2. Налаштувати журналювання.

3. Змінити сигнатури IPS.

4. Перевірити IPS.

**Результат виконання роботи**

**Частина 1. Увімкнути IOS IPS**

Крок 1. Увімкнути пакет Security Technology.

Перейдемо до налаштування пакету Security Technology на маршутизаторі R1. Спочатку виконаємо команду show version для перевірки інформації про ліцензію технологічного пакета. Як бачимо, пакет не встановлено.

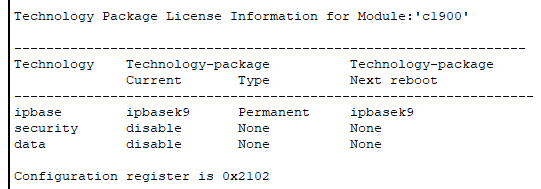
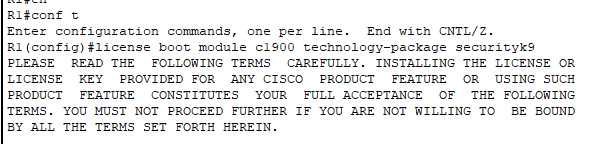


Рис.1. Перевірка ліцензії технологічного пакета

У режимі конфігурації скористаємось командою **# license boot module c1900 technology-package securityk9**. Приймаємо ліцензійну угоду кінцевого користвувача.



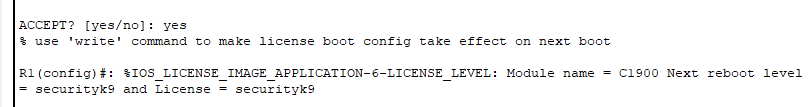


Рис.2. Увімкнення пакету Security Technology

Далі виходимо з режиму конфігурації, перезавантажуємо R1 зі збереженням поточної конфігурації (reload) та перевіряємо установку за допомогою команди show version. Як бачимо, у полі «security» з’явилось «securityk9».

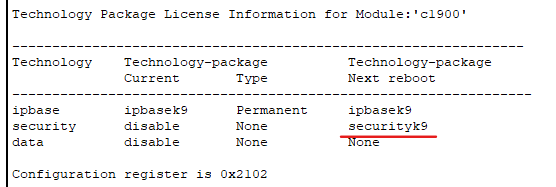


Рис.3. Перевірка установки ліцензії

Крок 2. Перевірка підключення до мережі.

Виконуємо пінгування з РС-С на РС-А. Пінг - успішний.

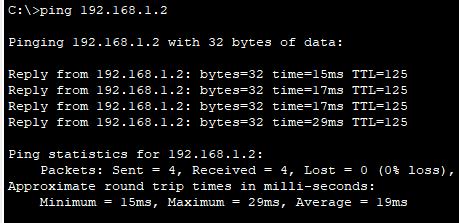


Рис.4. Пінгування з PC-C на PC-A

Виконуємо пінгування з РС-A на РС-C. Пінг - успішний.

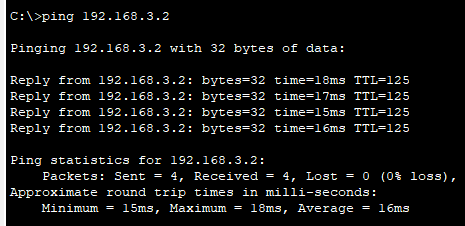


Рис.5. Пінгування з PC-C на PC-A

Крок 3. Створення каталогу конфігурації IOS IPS у Flash.

Переходимо до R1. Створюємо каталог флеш-пам’яті за допомогою команди **mkdir** з назвою **ipsdir**.

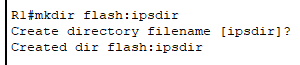


Рис.6. Створення каталогу ipsdir

Крок 4. Налаштування місця зберігання сигнатури IPS.

На R1 необхідно налаштувати місце зберігання сигнатури IPS як каталог (ipsdir). Спочатку входимо у режим конфігурації сигнатур **#ip ips config location**, і визначаємо каталог де будемо зберігати ips-сигнатури (**flash:ipsdir**). Після чого зберігаємо конфігурацію.



Рис.7. Налаштування місця зберігання IPS сигнатури

Крок 5. Створити правило IPS.

Cтворюємо назву правила IPS за допомогою команди # ip ips name iosips.



Рис.8. Створення правила IPS

Крок 6. Увімкнути журналювання.

Спочатку в режимі глобальної конфігурації вмикаємо syslog (# loggin on).



Рис.9. Увімкнення syslog

У режимі EXEC встановлюємо годинник на сьогоднішню дату.



Рис.10. Установка годинника

Переконаємося, що на R1 увімкнено службу часової позначки для журналювання за допомогою команди show run. Бачимо, що служби не увімкнені.



Рис.11. Перевірка служби часової позначки для журналювання

В режимі глобальної конфігурації вводимо наступні команди **(# service timestamps debug datetime msec** та # **service timestamps log datetime msec**) щоб ввімкнути відповідні служби.

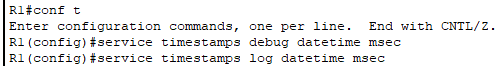


Рис.12. Увімкнення служби мітки часу та відлагодження

Надсилаємо повідомлення журналу на сервер syslog за IP-адресою 192.168.1.50.



Рис.13. Надсилання повідомлення журналу на сервер syslog

Крок 7. Налаштування IOS IPS для використання категорій сигнатур.

Перейдемо до режиму налаштування сигнатур IPS **(# ip ips signature-category**). Вилучаємо категорію всіх сигнатур (category all) за допомогою вилученої команди retired true. Скасуємо виведення базової категорії IOS\_IPS за допомогою вилученої команди retired false.

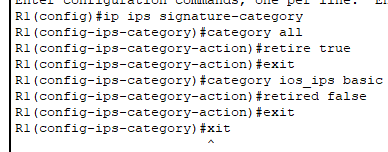


Рис.14. Налаштування IOS IPS

Крок 8. Застосувати правило IPS до інтерфейсу.

Необхідно застосувати правило IPS до інтерфейсу за допомогою команди ip ips name direction у режимі налаштування інтерфейсу. Застосуємо вихідне правило до інтерфейсу G0/1 R1. Після ввімкнення IPS деякі повідомлення журналу будуть надіслані на рядок консолі, вказуючи, що механізми IPS ініціалізуються.

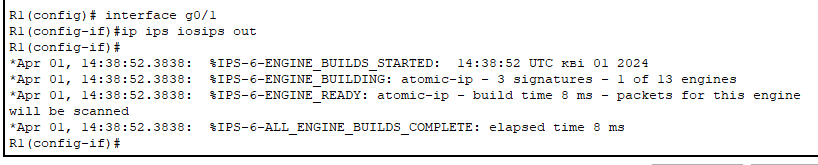


Рис.15. Застосування правила IPS до інтерфейса

**Частина 2. Внесення змін до сигнатури.**

Крок 1. Змінити подію-дію сигнатури.

Скасуємо сигнатуру ехо-запиту, увімкнемо його та змінимо дію сигнатури на сповіщення та видалення.

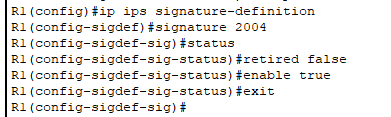


Рис.16. Зміна події-дії сигнатури

Крок 2. Використання команди show для перевірки IPS.

Використаємо команду show ip ips all, щоб переглянути підсумок стану конфігурації IPS.

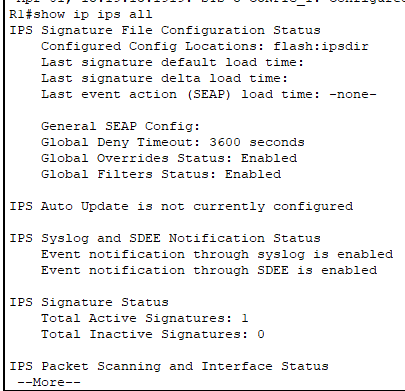


Рис.17. Перевірка IPS

Крок 3. Переконатися, що IPS працює належним чином.

З комп’ютера PC-C надіслаємо запит на комп’ютер PC-A. Результат – успішний.

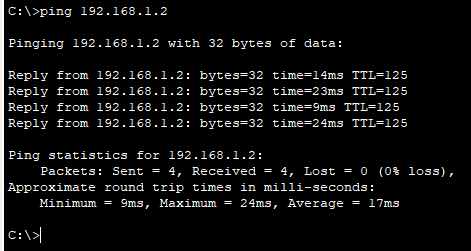


Рис.18. Надсилання запиту на PC-A з PC-C

З комп’ютера PC-A надіслаємо запит на комп’ютер PC-C. Результат – успішний.

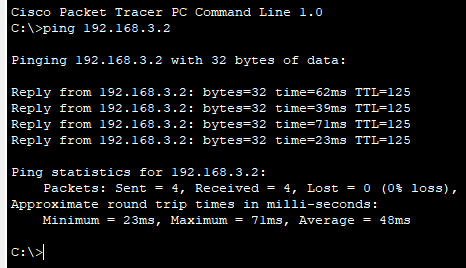


Рис.19. Надсилання запиту на PC-C з PC-A

Крок 4. Переглянути повідомлення Syslog журналу.

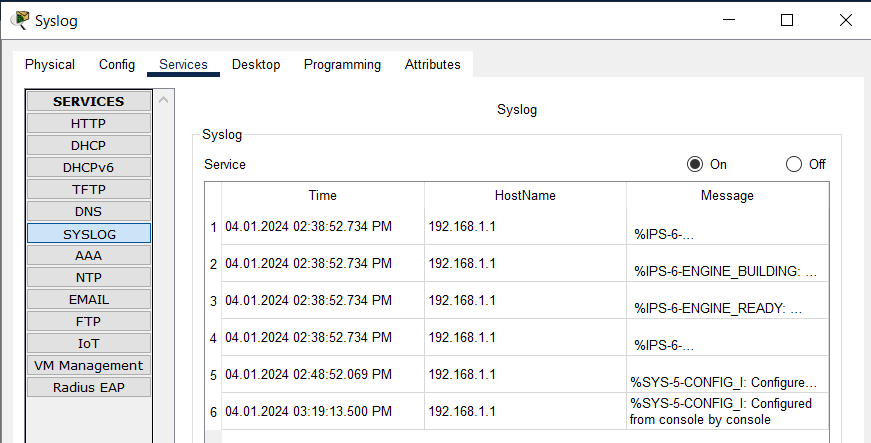


Рис.20. Перевірка SYSLOG журналу на сервері

Крок 5. Перевірка результатів.

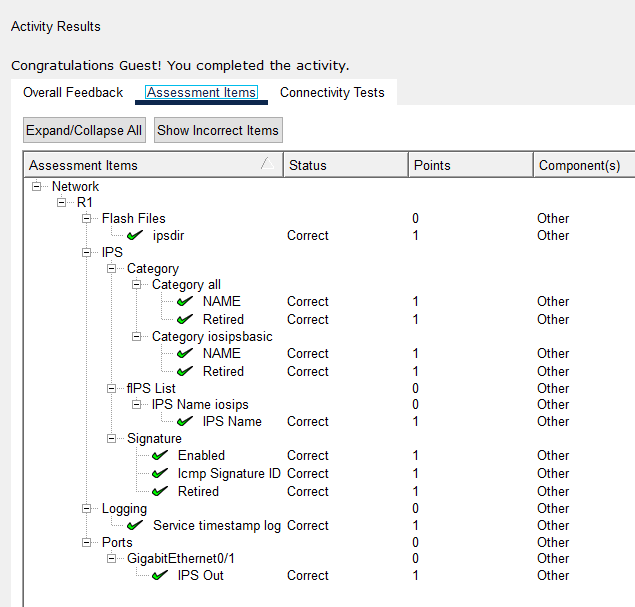


Рис.21. Перевірка результату виконання

**Висновок:**

У результаті виконання лабораторної роботи було опрацьовано особливості налаштування функціонування системи запобігання вторгненням IOS (IPS) за допомогою CLI; увімкнено ISO IPS та змінено сигнатуру IPS, а також налаштовано журналювання.