### Задание 19.6.1 (HW-03)

**Персонализация:** Михайлов Юрий Никитич (uramihajlov481@gmail.com)

**Лабораторная работа:** Задание**№**19.6.1 (HW-03)**:**

Общая информация:

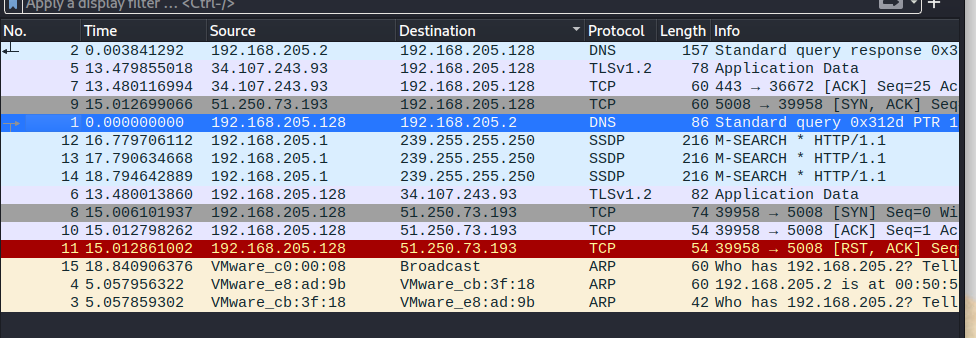
* Период тестирования: 28.03.2024
* Объект тестирования: http://51.250.73.193:5008
* Описание действий:

**Задачи:**Протестировать как можно больше ключей для nmap типа:

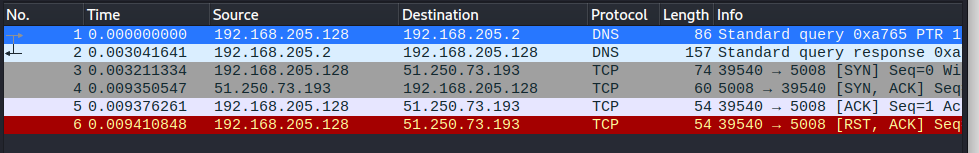
* **-T (от T1 до T6),**
* **-sS, -sT, -sA, -sW, -sM — применять разные типы сканирования, смотреть на их отличия в трафике,**
* **-sV — посмотреть, как nmap будет определять версии,**
* **-A.**

**1) -T (от T1 до T6):** Этот ключ устанавливает скорость сканирования. Возможные значения от T1 до T6, где T1 - наименее агрессивное и T6 - наиболее агрессивное сканирование. Более высокие значения увеличивают скорость сканирования, но также могут увеличить вероятность обнаружения как инструмента сканирования, так и увеличить риск ложных срабатываний.

**nmap -Pn -p -T1 5008 51.250.73.193**



**nmap -Pn –T4 -p5008 51.250.73.193**

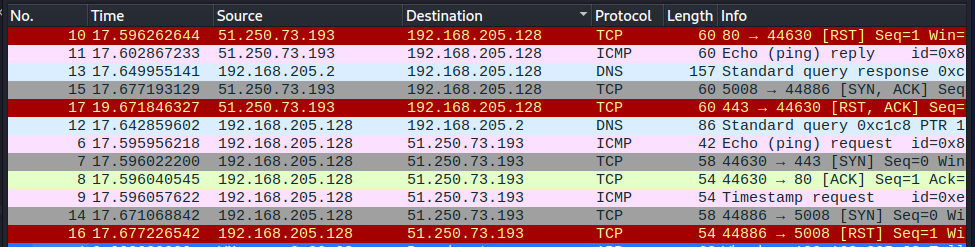


**2)** **-sS**, **-sT**, **-sA**, **-sW**, **-sM**: Эти ключи определяют тип сканирования.

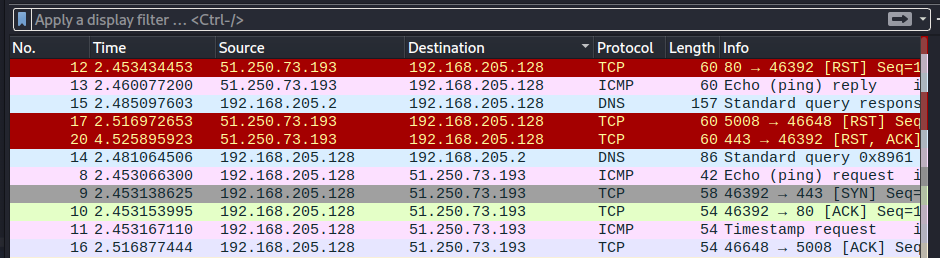
* **-sS**: TCP SYN сканирование.
* **-sT**: TCP Connect сканирование.
* **-sA**: ACK сканирование.
* **-sW**: Window сканирование.
* **-sM**: Maimon сканирование.

Каждый из этих типов сканирования имеет свои особенности, например, TCP SYN сканирование (-sS) позволяет определить открытые порты, отправляя SYN пакеты и анализируя ответы.

**nmap -sS -p5008 51.250.73.193**

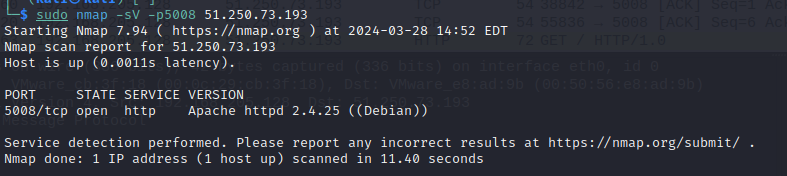


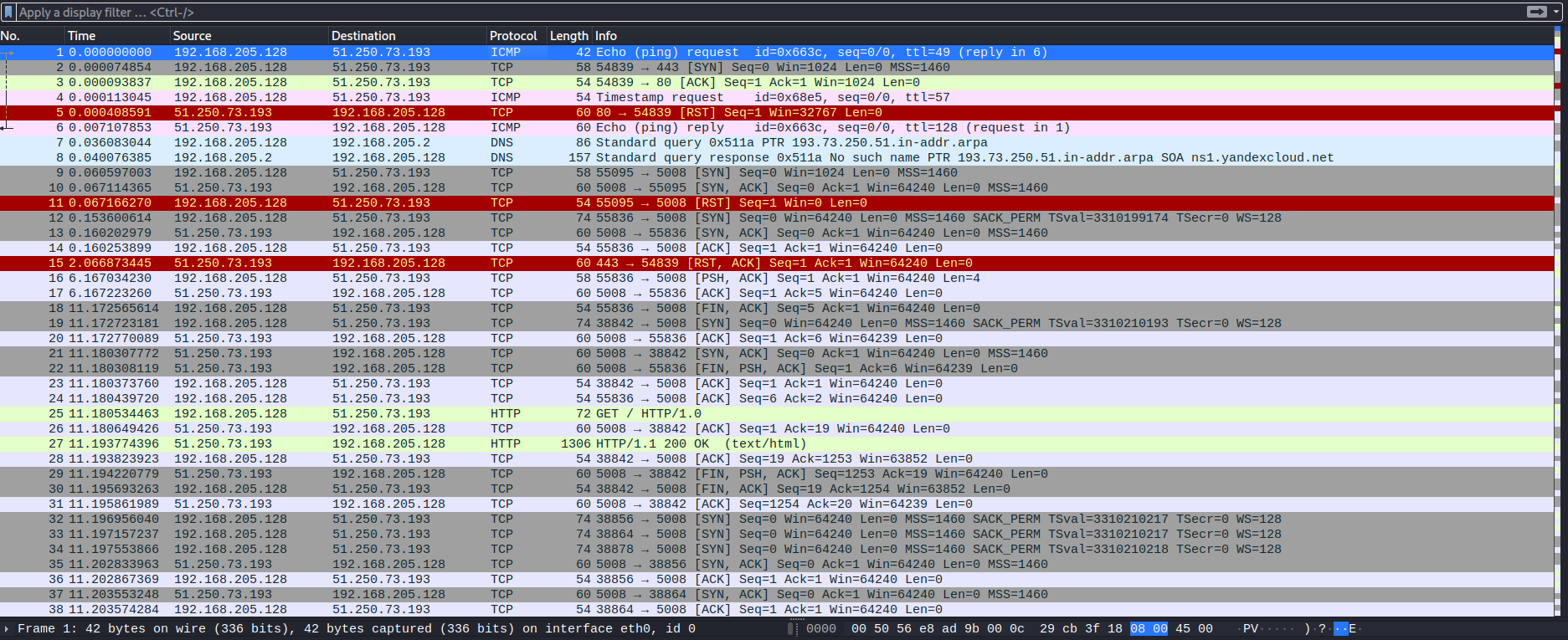
**nmap -sW -p5008 51.250.73.193**

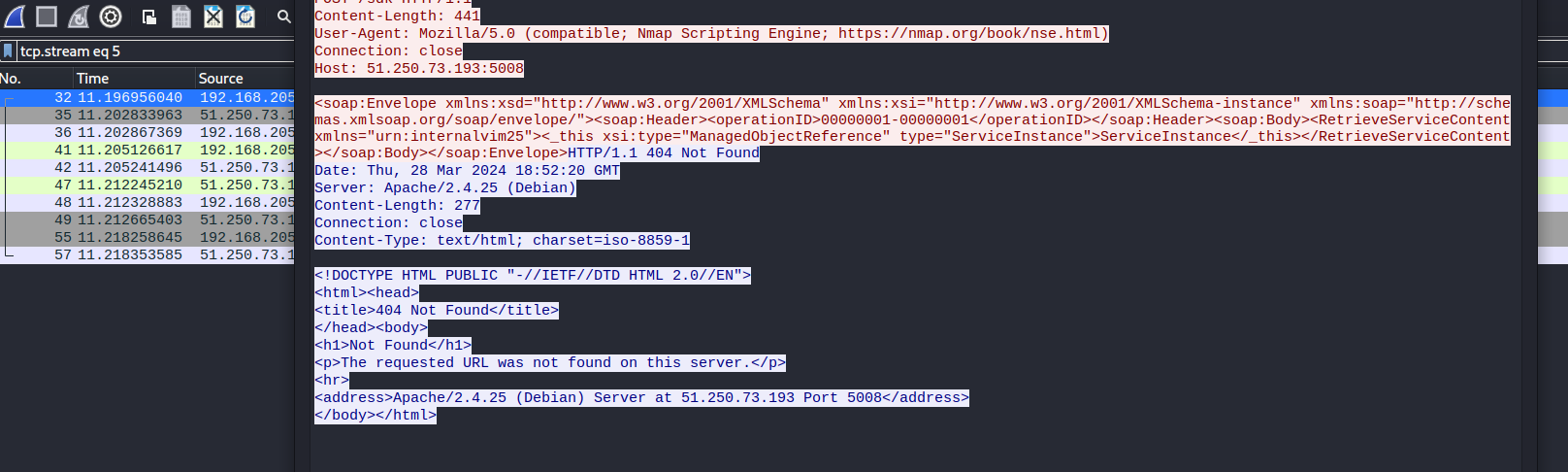


**3)** **-sV**: Этот ключ позволяет определить версии сервисов, работающих на открытых портах. Он сканирует порты, а затем пытается определить версии сервисов по их ответам.

**nmap -sV -p5008 51.250.73.193**

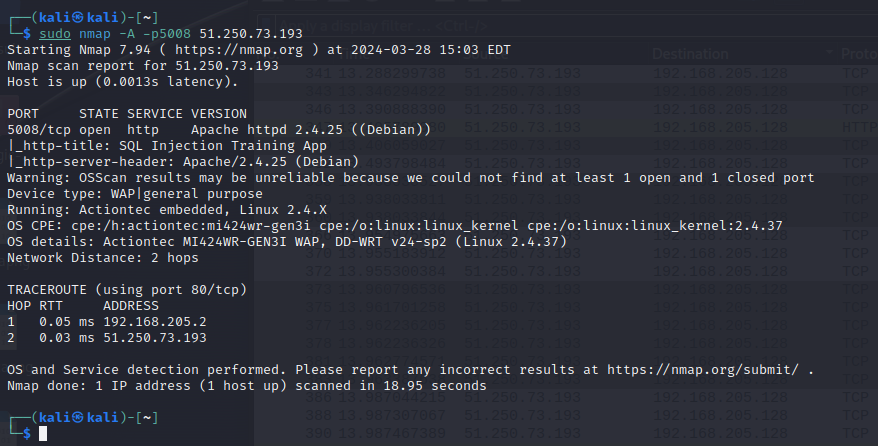
****

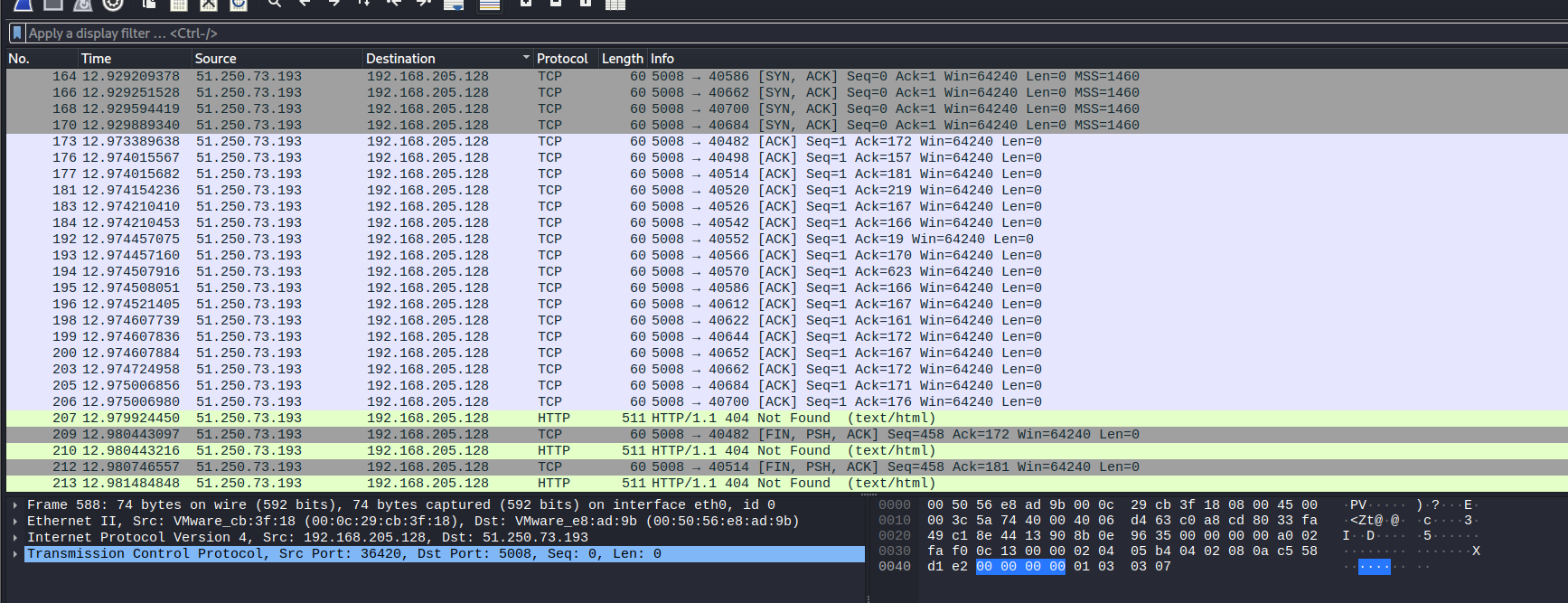




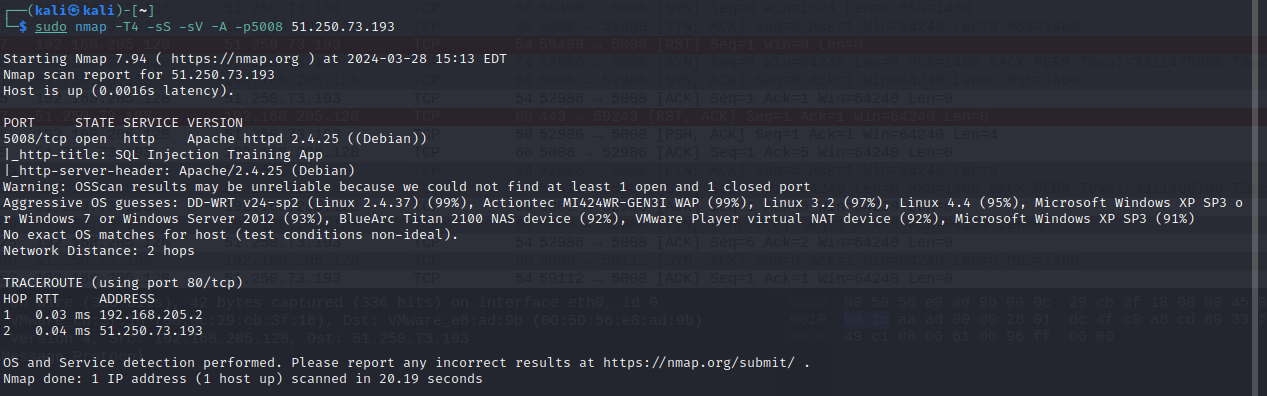
**4) -A:** Этот ключ запускает агрессивное сканирование, включая определение версий (-sV), сканирование операционной системы (-O), трассировку маршрута (-traceroute) и многое другое. Это удобно, когда вы хотите получить максимальное количество информации о целевой системе.

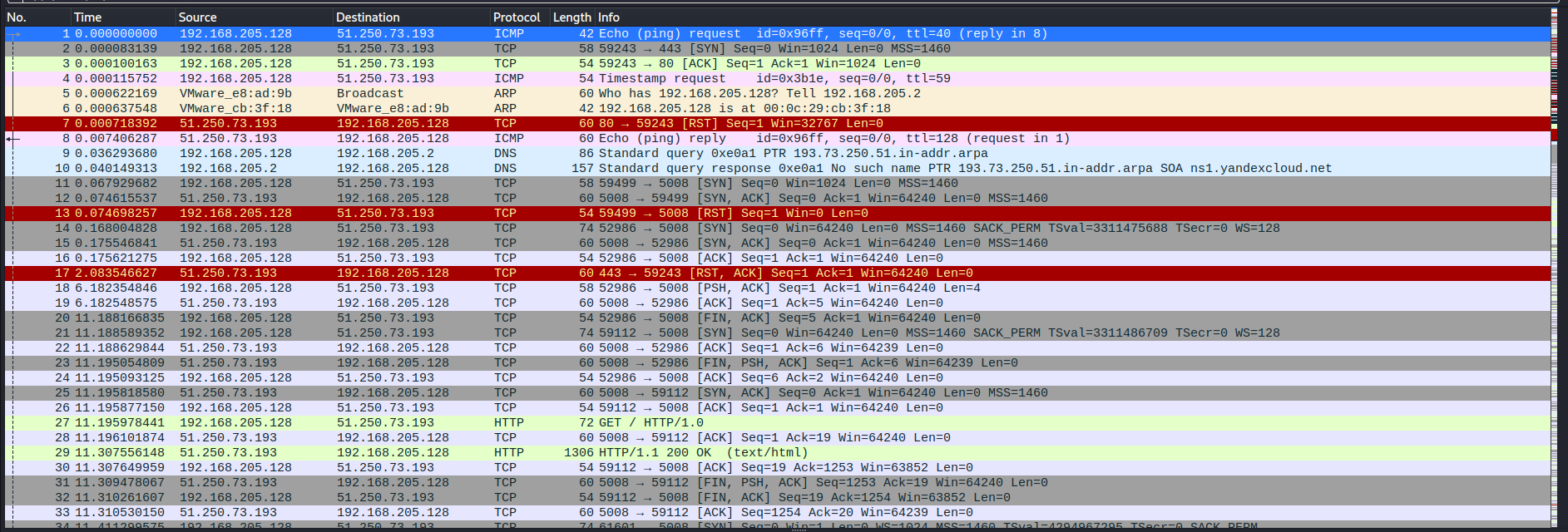
**Sudo nmap -A -p5008 51.250.73.193**

****

****

**5) Смесь ключей  
  
nmap -T4 -sS -sV -A -p 5008 51.250.73.193**

****

****

**Вывод:**

1. TCP SYN сканирование (-sS):
   * Положительные стороны: Быстрое сканирование, обнаружение открытых портов.
   * Ограничения: Может быть обнаружено средствами защиты, такими как сетевые брандмауэры.
2. Определение версий сервисов (-sV):
   * Положительные стороны: Позволяет определить версии сервисов, запущенных на открытых портах.
   * Ограничения: Может быть медленным при сканировании большого количества портов.
3. Агрессивное сканирование (-A):
   * Положительные стороны: Включает в себя определение версий, сканирование операционной системы, трассировку маршрута и другие полезные функции.
   * Ограничения: Может быть медленным и вызывать повышенное внимание средств безопасности.
4. Установка скорости сканирования (-T4):
   * Положительные стороны: Ускоряет сканирование приемлемой для большинства сетей скоростью.
   * Ограничения: Может привести к более высокой нагрузке на сеть и вызвать блокировку в случае детекции.