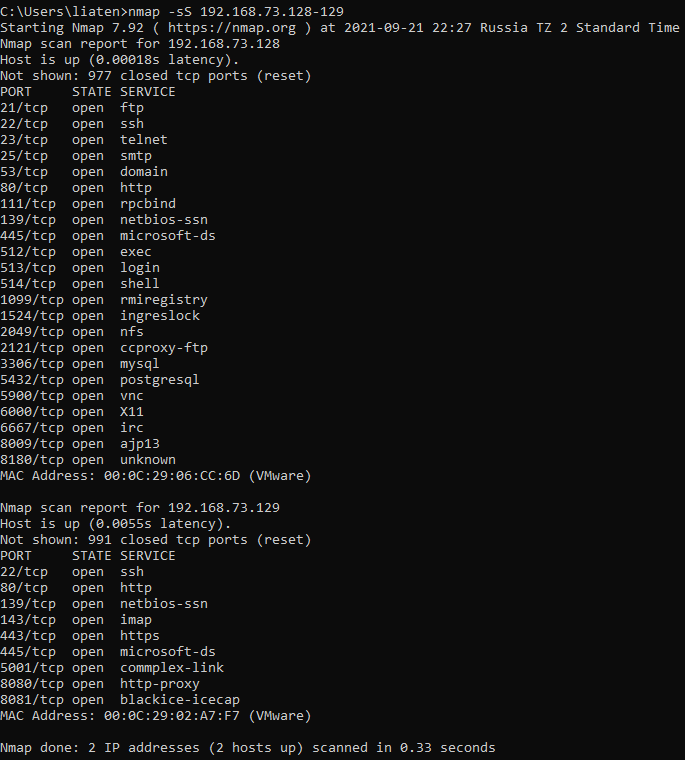
**Практика.** Сканирование портов и служб

В прошлом задании мы идентифицировали две машины, теперь давайте узнаем какие у них есть порты. Начнём с UDP сканирования, оно занимает больше времени чем TCP сканирование.

1. Запускаем сканирование nmap, в командной строке введем **nmap -sU 192.168.73.128-129.** (адреса для сканирования мы определили в прошлом задании). Сканирование займет какое-то время.



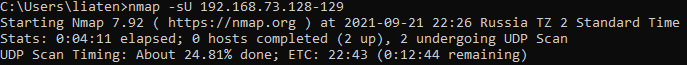
1. Не будем терять время и запустим еще одну Командную строку (зажмите Shift и нажмите на иконку запущенной Командной строки) и проведём скрытое TCP сканирование. Запустим команду **nmap -sS 192.168.73.128-129**. Сканирование практически сразу выдаст нам результат.



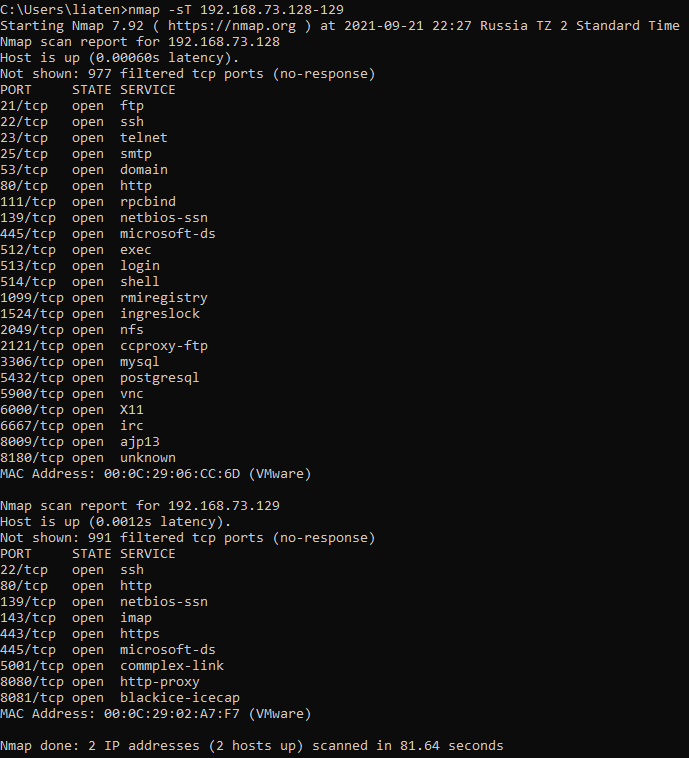
1. Естественно, система обнаружила множество открытых портов, это связано с тем, что наши машины специально подготовлены для эксплуатации уязвимостей, на реальных целях открытых портов будет гораздо меньше.
2. Давайте теперь попробуем провести **TCP сканирование с соединением**, введем **nmap -sT 192.168.73.128-129**. На это уйдет чуть больше времени.

*Тем временем наше UDP сканирование всё еще работает, оно очень долгое. Когда завершится сканирование с соединением, мы проведем сканирование служб на TCP портах. По умолчанию* ***nmap*** *сканирует только тысячу портов, а всего их 65536, мы могли бы просканировать их все, но это бы заняло очень много времени.*

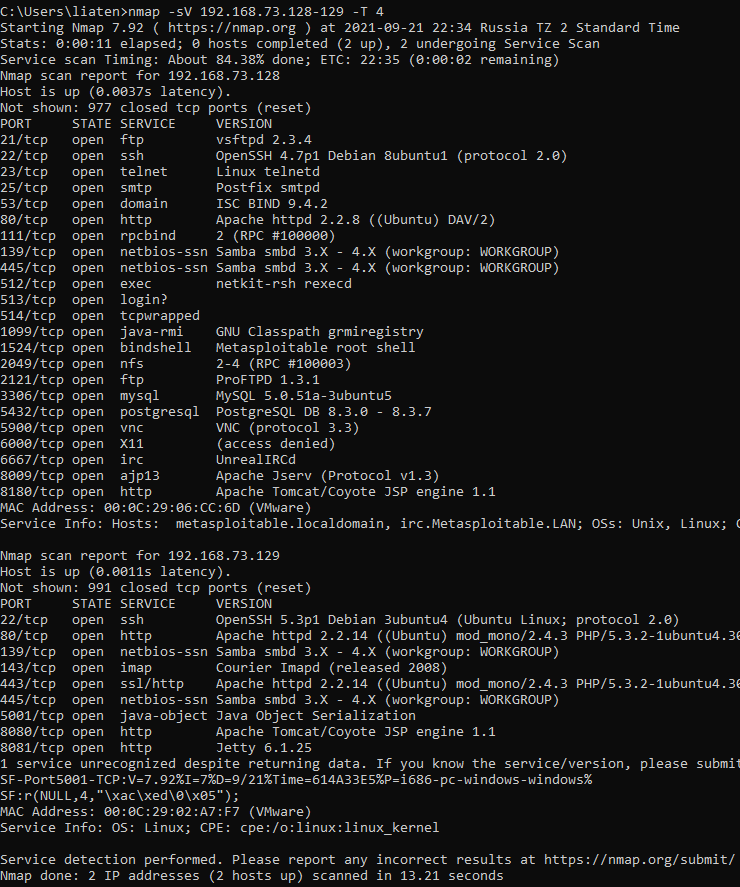
1. Пока ждём результата сканирования, можете нажать на пробел в консоли, и вы увидите % проделанного сканирования. Да, сканирование занимает много времени. Если бы к запросу мы добавили ключ **-v**, мы бы видели результаты в live-режиме.



1. Ура, мы получили результаты нашего **TCP сканирование с соединением**, мы получили два новых порта относительно **скрытого TCP сканирования**, со статусом “фильтруется”.

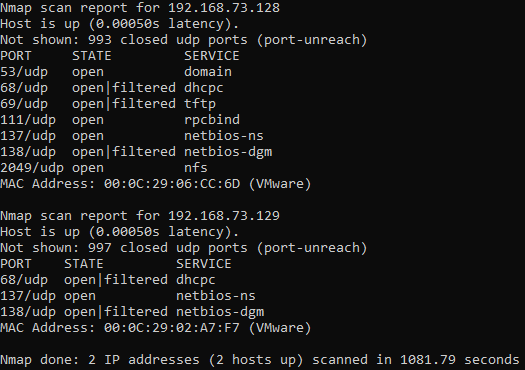


1. Теперь давайте запустим сканирование служб, командой **nmap -sV 192.168.73.128-129 -T 4.** Параметр -T называется таймингом, T5 - самый быстрый вариант сканирования, выберем T4. И довольно быстро получаем результат:



1. Мы нашли Apache Tomcat, OpenSSH 5.3p1, версию PHP и Python, Samba smbd и др. Это даёт нам возможность более детально подготовится к атаке на эти машины.
2. Тем временем завершилось наше UDP сканирование, мы видим результат.





1. Мы видим, что на 53 порту работает служба доменных имен, на 68 и 69 порту мы получили молчание, значит они либо открыты без службы, либо фильтруются.

На этом мы заканчиваем со сканированием портов и служб, переходим к оценке и идентификации уязвимостей.