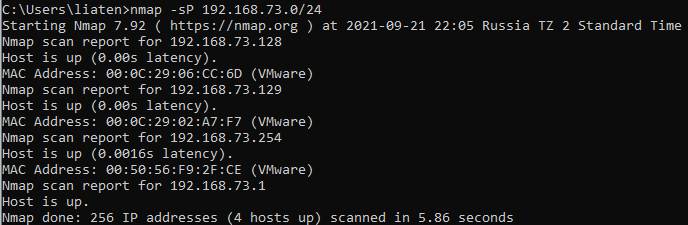
Практика. Поиск живых систем

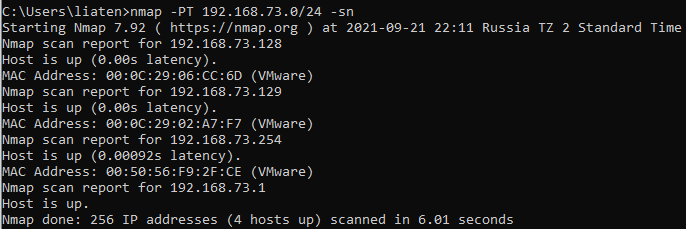
1. Запустим подготовленные ранее виртуальные машины Metasploitable2 и OWASP Broken Web и наш nmap установленный на хостовой машине. Давайте составим таблицу наших гостевых систем, чтобы небыло путанницы. У вас будут другие IP адреса.

|  |  |  |  |
| --- | --- | --- | --- |
| Гостевая система | IP адрес | Логин | Пароль |
| Metasploitable2 | 192.168.73.128 | msfadmin | msfadmin |
| OWASP Broken Web | 192.168.73.129 | root | owaspbwa |

1. Первый тип скнаированированя который мы будем проводить, это ping sweep (пинг свип). С помощью него отправляются **ICMP** пакеты и ожидается ответ от цели. Проведем данный запрос через nmap на сеть, в которой расположены наши гостевые системы, в моём случае это 192.168.73.0/24.
2. Запускаем Командную строку и вводим команду **nmap -sP 192.168.73.0/24**. Параметр **-sP** говорит о том, что мы будем отправлять **ICMP пакет**.



1. В результате сканирования мы получили цели, 192.168.73.1 и 192.168.73.254 — это виртуальные свитчи VMware, они нас не интересуют. Мы определили, что у нас есть две цели, с адресами 192.168.73.128 и 192.168.73.129. (Естественно мы знаем, что это за цели, данный пример сэмулировал специально, чтобы показать, как проводить поиск целей).
2. Не всегда данный запрос пройдёт, зачастую его просто отфильтрует межсетевой экран. Давайте проведём TCP сканирование. **nmap -PT 192.168.86.0/24 -sn.** Параметр **-PT** говорит о том, что мы будем отправлять TCP-запрос, а параметр **-sn** говорит о том, что не нужно сканировать порты исследуемых целей.



1. Результат такой же, как и в первом примере, но если бы в сети были, к примеру, Windows с включенным межсетевым экраном, первый запрос не обнаружил бы эту систему.