## Методы "невидимого" удаленного сканирования

Для работы нам понадобится вручную генерировать icmp пакеты, в этом нам поможет утилита hping3

|  |
| --- |
| hping3 192.168.66.20 -r |

в wireshark посмотрите что identification изменился на 1

tcp отправляет с 0 порта

Будем сканировать DVL.

посмотрим в DVL сетевые интерфейсы и открытые порты.

|  |
| --- |
| ifconfig netstat -nltp |

далее в качестве немого хоста у нас Windows 7

в качестве сканируемого узла DVL

Формат

hping3 [кого сканируем] -a [исходный адрес] -p [порт] -S (используем SYN флаг)

|  |
| --- |
| hping3 192.168.88.1 -a 192.168.88.253 -p 3306 -S |

|  |
| --- |
| hping3 192.168.88.1 -a 192.168.88.253 -p 1000 -S |

и смотрим на результаты hping3

Можно сделать ту же атаку и с помощью nmap

|  |
| --- |
| nmap -Pn -sI 192.168.66.20 192.168.88.251 |

используя 192.168.66.20

#### Сканирование сервисов

Пример

|  |
| --- |
| nmap -n -sS -sV scanme.nmap.org |

нужно подождать

Как nmap распознает сервисы?

по тому, как отвечают сервисы на запросы.

Экспресс тесты, либо из заголовков если сами сервисы сами рассказывают

Если, например на 192.168.88.1 установлен telnet уже сам telnet расскажет много интересного

|  |
| --- |
| telnet 192.168.88.1 |

Такой подход позволяет сканировать ОС, версию ядра.

#### Еще примеры сканирования

##### Уязвимость в настройках mysql

в DVL

|  |
| --- |
| mysql GRANT ALL PRIVILEGES ON \*.\* TO 'root'@'%' IDENTIFIED BY '' WITH GRANT OPTION; exit |

запускаем в Kali nmap со скриптом на поиск пустого пароля

|  |
| --- |
| nmap -sV --script=mysql-empty-password 192.198.66.21 map -p 3306 192.168.88.251 --script mysql-query --script-args='qoery-"select 1;",username-root' |