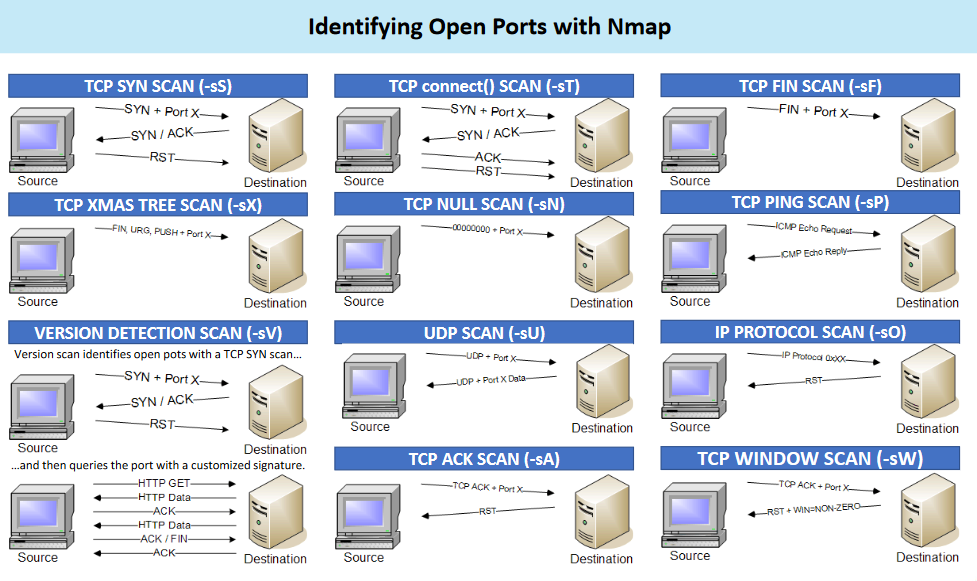
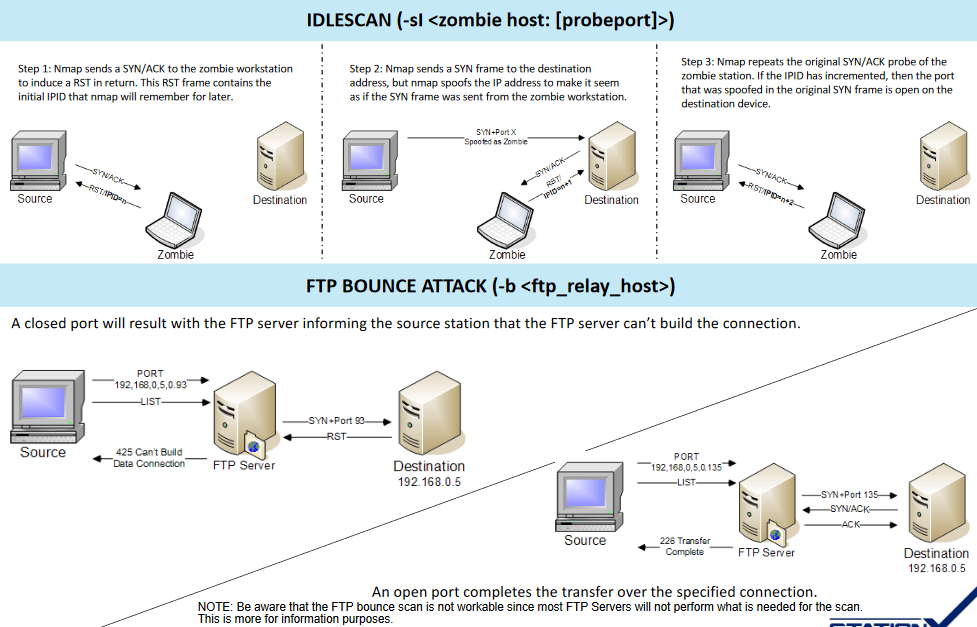
|  |  |  |
| --- | --- | --- |
| **NMAP** | | |
| **Спецификация объектов:** | | |
| **Флаг** | **Пример** | **Описание** |
|  | nmap 192.168.1.1 | сканирование одного IP |
|  | nmap 192.168.1.1 192.168.2.1 | сканирование определенных IP |
|  | nmap 192.168.1.1-254 | сканирование диапазона |
|  | nmap scanme.nmap.org | сканирование домена |
|  | nmap 192.168.1.0/24 | сканирование по адресу маски (CIDR) |
| **-iL** | nmap -iL targets.txt | сканирование объекта из файла target.txt |
| **-iR** | nmap -iR 100 | сканирование 100 случайных хостов |
| **--exclude** | nmap --exclude 192.168.1.1 | исключить перечисленные хосты |
| **Методы сканирования:** | | |
| **Флаг** | **Пример** | **Описание** |
| **-sS** | nmap 192.168.1.1 -sS | TCP SYN port scan (По умолчанию) |
| **-sT** | nmap 192.168.1.1 -sT | TCP connect port scan (По умолчанию без привилегий root) |
| **-sU** | nmap 192.168.1.1 -sU | UDP port scan |
| **-sA** | nmap 192.168.1.1 -sA | TCP ACK port scan |
| **-sW** | nmap 192.168.1.1 -sW | TCP Window port scan |
| **-sM** | nmap 192.168.1.1 -sM | TCP Maimon port scan |
| **Обнаружение хостов:** | | |
| **Флаг** | **Пример** | **Описание** |
| **-sL** | nmap 192.168.1.1-3 -sL | никакого сканирования, только перечисление объектов |
| **-sn** | nmap 192.168.1.1/24 -sn | отключение сканирования портов, только обнаружение хостов |
| **-Pn** | nmap 192.168.1.1-5 -Pn | отключение обнаружения хостов, только сканирование портов |
| **-PS** | nmap 192.168.1.1-5 -PS22-25,80 | обнаружение TCP SYN на порту X (по умолчанию 80) |
| **-PA** | nmap 192.168.1.1-5 -PA22-25,80 | обнаружение TCP ACK на порту X (по умолчанию 80) |
| **-PU** | nmap 192.168.1.1-5 -PU53 | UDP исследование на порту Х (по умолчанию 40125) |
| **-PR** | nmap 192.168.1.1-1/24 -PR | ARP обнаружение в локальной сети |
| **-n** | nmap 192.168.1.1 -n | Нет резолва обратных IP адрессов |
| **Спецификация портов:** | | |
| **Флаг** | **Пример** | **Описание** |
| **-p** | nmap 192.168.1.1 -p 21 | сканирование портов на порту Х |
| **-p** | nmap 192.168.1.1 -p 21-100 | диапазон портов |
| **-p** | nmap 192.168.1.1 -p U:53,T:21-25,80 | сканирование нескольких портов TCP, UDP |
| **-p-** | nmap 192.168.1.1 -p- | сканирование всех портов |
| **-p** | nmap 192.168.1.1 -p http,https | сканирование портов из имени службы |
| **-F** | nmap 192.168.1.1 -F | быстрое сканирование портов (100 портов) |
| **--top-ports** | nmap 192.168.1.1 –top-ports 2000 | сканирование top портов в Х портах |
| **-p-65535** | nmap 192.168.1.1 -p-65535 | оставляя начальный порт в диапазоне,  запускает сканирование с порта 1 |
| **-p0-** | nmap 192.168.1.1 -p0- | выходя из конечного порта в диапазоне, делает сканирование проходящим через порт 65535 |
| **Обнаружение служб и версий:** | | |
| **Флаг** | **Пример** | **Описание** |
| **-sV** | nmap 192.168.1.1 -sV | попытка определить версию службы, работающей на порту |
| **-sV --version-intensity** | nmap 192.168.1.1 -sV –version-intensity 8 | уровень интенсивности от 0 до 9. Большее число увеличивает вероятность правильности |
| **-sV --version-light** | nmap 192.168.1.1 -sV –version-light | включает световой режим. Более низкая вероятность правильности. Быстрее |
| **-sV --version-all** | nmap 192.168.1.1 -sV –version-all | включает уровень интенсивности 9. Более высокая вероятность правильности. Медленнее |
| **-A** | nmap 192.168.1.1 -A | включает определение ОС, версию обнаружения, сканирование с использованием скриптов и трассировки. Это агрессивное сканирование – включает в себя -sV, -O, --traceroute, использование скриптов |
| **Обнаружение ОС:** | | |
| **Флаг** | **Пример** | **Описание** |
| **-O** | nmap 192.168.1.1 -O | Удаленное обнаружение ОС с помощью TCP/IP  stack fingerprinting |
| **-O --osscan-limit** | nmap 192.168.1.1 -O --osscan-limit |  |
| **-O --osscan-guess** | nmap 192.168.1.1 -O --osscan-guess | делает NMAP угадывание более агрессивным |
| **-O --max-os-tries** | nmap 192.168.1.1 -O –max-os-tries 1 |  |
| **-A** | nmap 192.168.1.1 -A | включает определение ОС, версию обнаружение, сканирование с использованием скриптов и трассировки |
| **Сроки и производительность:** | | |
| **Флаг** | **Пример** | **Описание** |
| **-T0** | nmap 192.168.1.1 -T0 | параноидальная, используется для обхода IDS |
| **-T1** | nmap 192.168.1.1 -T1 | скрытая, используется для обхода IDS |
| **-T2** | nmap 192.168.1.1 -T2 | вежливая, замедляет сканирование для использования меньшей пропускной способности и меньших машинных ресурсов |
| **-T3** | nmap 192.168.1.1 -T3 | нормальная, является скоростью по умолчанию |
| **-T4** | nmap 192.168.1.1 -T4 | агрессивная, предполагается, что сканирование производится в быстрой и надежной сети |
| **-T5** | nmap 192.168.1.1 -T5 | безумная скорость сканирования, предполагается, что сканирование производится в необычайно быстрой сети |
| **NSE Скрипты:** | | |
| **Флаг** | **Пример** | **Описание** |
| **-sC** | nmap 192.168.1.1 -sC | сканирование с помощью сценариев NSE по умолчанию. Считается полезным для обнаружения и безопасным |
| **--script default** | nmap 192.168.1.1 --script default | сканирование с помощью сценариев NSE по умолчанию. Считается полезным для обнаружения и безопасным |
| **--script** | nmap 192.168.1.1 --script=banner | сканирование с помощью одного скрипта. Пример баннера |
| **--script** | nmap 192.168.1.1 --script=http\* | сканирование с помощью подстановочного знака. Пример http |
| **--script** | nmap 192.168.1.1 --script=http,banner | сканирование с помощью двух сценариев. Пример http и баннер |
| **--script** | nmap 192.168.1.1 --script “not intrusive” | сканируйте по умолчанию, но удаляйте навязчивые скрипты |
| **--script-args** | nmap --script snmp-sysdescr --script-args snmpcommunity=admin 192.168.1.1 | скрипт NSE с аргументами |
| **Firewall / IDS - Уклонение и Cпуфинг:** | | |
| **Флаг** | **Пример** | **Описание** |
| **-f** | nmap 192.168.1.1 -f | запрошенное сканирование (включая сканирование ping), использует крошечные фрагментированные IP-пакеты. Сложнее для пакетных фильтров |
| **--mtu** | nmap 192.168.1.1 --mtu 32 | задайте ваш собственный размер |
| **-D** | nmap -D 192.168.1.101,192.168.1.102, 192.168.1.103,192.168.1.23 | отправка сканирований с поддельных IP-адресов |
| **-D** | nmap -D decoy-ip1,decoy-ip2,your-own-ip,decoy-ip3,decoy-ip4 remote-host-ip |  |
| **-S** | nmap -S www.microsoft.com www.facebook.com | сканирование Facebook от Microsoft (может потребоваться-e eth0 -Pn) |
| **-g** | nmap -g 53 192.168.1.1 | используйте заданный номер порта источника |
| **--proxies** | nmap --proxies http://192.168.1.1:8080, http://192.168.1.2:8080 192.168.1.1 | реле подключения через прокси http/SOCKS4 |
| **--data-length** | nmap --data-length 200 192.168.1.1 | дописывает случайную информацию в отправленные пакеты |
| **Выход (Output):** | | |
| **Флаг** | **Пример** | **Описание** |
| **-oN** | nmap 192.168.1.1 -oN normal.file | нормальный вывод в файл в normal.file |
| **-oX** | nmap 192.168.1.1 -oX xml.file | вывод XML в файл xml.файл |
| **-oG** | nmap 192.168.1.1 -oG grep.file | grepable выводится в файл grep.файл |
| **-oA** | nmap 192.168.1.1 -oA results | вывод данных сразу в трех основных форматах |
| **-oG-** | nmap 192.168.1.1 -oG - |  |
| **--append-output** | nmap 192.168.1.1 -oN file.file --append-output | добавление сканирования к предыдущему файлу сканирования |
| **-v** | nmap 192.168.1.1 -v | увеличивает уровень детализации (использовать -vv или больше для большего эффекта) |
| **-d** | nmap 192.168.1.1 -d | увеличивает уровень отладки (использовать -dd или больше для большего эффекта) |
| **--reason** | nmap 192.168.1.1 --reason | отображение причины, по которой порт находится в определенном состоянии, тот же вывод, что и -vv |
| **--open** | nmap 192.168.1.1 --open | показывать только открытые (или возможно открытые) порты |
| **--packet-trace** | nmap 192.168.1.1 -T4 --packet-trace | показать все отправленные и полученные пакеты |
| **--iflist** | nmap --iflist | показывает интерфейсы хоста и маршруты |
| **--resume** | nmap --resume results.file | возобновление сканирования |
| **Прочие опции:** | | |
| **Флаг** | **Пример** | **Описание** |
| **-6** | nmap -6 2607:f0d0:1002:51::4 | включить сканирование IPv6 |
| **-р** | nmap -h | nmap help screen |
| **Другие Полезные Команды Nmap:** | | |
| **Команда** | | **Описание** |
| nmap -iR 10 -PS22-25,80,113,1050,35000 -v -sn | | обнаружение только на портах Х, без сканирования портов |
| nmap 192.168.1.1-1/24 -PR -sn -vv | | ARP обнаружение только в локальной сети, без сканирования портов |
| nmap -iR 10 -sn -traceroute | | трассировка к случайным целям, без сканирования портов |
| nmap 192.168.1.1-50 -sL --dns-server 192.168.1.1 | | запрашивает внутренний DNS для хостов, перечисляет только целевые объекты |



**TCP connect() SCAN (-sT**) используется крайне редко поскольку при полноценном установлении соединения запись об установленном соединении помечается в логах.

**Статья о различных методах сканирования через nmap (с примерами из Wireshark):**

<https://easy-network.ru/poleznoe/100-skanirovanie-portov-s-nmap.html#port-zakryt-4>

--script=vuln использование NSE скриптов nmap для поиска уязимостей



nmap -sS -p0-65535 -sV 10.10.10.120 --script=vuln