nmap

Несколько полезных опций:

- -P0 – Не пинговать хост перед сканированием. Полезно в случаях, когда ICMP- игнорируются сервером.
- -O – Позволяет задействовать систему определения OS fingerprints, иногда полезно знать, на какой оси работает компьютер.
- -v – Вербализация. Очень полезная штука – выдает гораздо больше информации о том, что было обнаружено при сканировании.
- -o <имя файла> – Позволяет задать имя файла, куда будут записаны результаты сканирования.
- -p <порт/порты> – Опция, с помощью которой можно задавать конкретный номер сканируемого порта или же диапазон портов. Например, -p 23, -p 1-105 и так далее. По умолчанию просматривается диапазон с первого по 1024 порт.
- -F – При сканировании рассматриваются только те порты, которые внесены в вышеупомянутый список “известных сервисов”. Эта опция существенно ускоряет процесс сканирования.

Способы задачи адресов:

1. 192.168.1.1 – прямой
2. 192.168.*.* – по маске
3. 192.168.0-255.0-255 – диапазон
4. 192.168.1-50,51-255.1,2,3,4,5-255 – диапазоны
5. 192.168.0.0/16 – сабнет (для сетей класса C используется маска /24)

Пример стандартного сканирования одного хоста, с определением версии операционной системы, повышенной вербализацией и записью в лог файл:

```
# nmap -sS -O -v -o scan_host.log host.com
```