

Nmap

- Nmap 是 Linux 系统特有的命令，可以进行网络扫描。
 - 我们将要尝试用 Nmap 扫描学校的网络
- 在命令行执行
 - `nmap -O 127.1`
- 注意类似这样的信息
 - Running: Linux 3.X|4.X



Nmap

- 语法
 - `sudo nmap -O IP 地址` # 'O' 是大写的
 - # 这个命令可以扫描某个 IP 地址的操作系统
- 举例
 - `sudo nmap -O 172.17.0.21`
 - # 172.17.0.21 是 HCC 服务器的 IP



数据流重导向

- 符号
 - 程序 < 文件
 - 程序 << 字符串
 - 程序 > 文件
 - 程序 >> 文件
 - 程序 2> 文件
 - 程序 &> 文件
- 提示
 - 将 stdin 换为文件
 - 指定 EOF 为字符串
 - 将 stdout 导向到文件
 - 追加模式
 - stderr
 - stderr + stdout

open

- open 可以打开文件
 - `open('a.txt', 'w')` # 打开文件，写入模式
 - `a.write('hello')` # 写入文字
 - `a.close()` # 关闭
 - `open('a.txt').read()` # 读取



os.system

- os 是一个和系统有关的模块
 - 使用这句话引用
 - `import os`
 - 试一试 `help`
- `os.system(cmd)`
 - # cmd 是一条命令
- `os.walk(dir)`
 - # dir 是一个目录
- 更多
 - <https://docs.python.org/3/library/os.html>

下次活动的任务

- 通过 Python 编程控制 Nmap 扫描学校的网络
 - 网络地址是 10.bbb.ccc.ddd
 - bbb 大约在 0~64 以内
 - ccc 大约在 0~64 以内
 - ddd 在 1~254 以内