参考：
http://www.youknowi.xin/2018/08/nmap%e8%84%9a%e6%9c%ac%e5%88%a9%e7%94%a8%e7%af%87/

有爆破，历史漏洞验证，版本探测，端口扫描，特定服务的扫描等

其实讲道理，目前个人只用了 script-vuln 这个脚本，其他的脚本用专门的工具可能效果要更好一点

0x01 nmap 按脚本分类扫描

nmap 脚本主要分为以下几类，在扫描时可根据需要设置--script=类别这种方式进行比较笼统的扫描：

auth: 负责处理鉴权证书（绕开鉴权）的脚本

broadcast: 在局域网内探查更多服务开启状况，如 dhcp/dns/sqlserver 等服务

brute: 提供暴力破解方式，针对常见的应用如 http/snmp 等

default: 使用-sC 或-A 选项扫描时候默认的脚本，提供基本脚本扫描能力

discovery: 对网络进行更多的信息，如 SMB 枚举、SNMP 查询等

dos: 用于进行拒绝服务攻击

exploit: 利用已知的漏洞入侵系统

external: 利用第三方的数据库或资源，例如进行 whois 解析

fuzzer: 模糊测试的脚本，发送异常的包到目标机，探测出潜在漏洞 intrusive: 入侵性的脚本，此类脚本可能引发对方的 IDS/IPS 的记录或屏蔽

malware: 探测目标机是否感染了病毒、开启了后门等信息

safe: 此类与 intrusive 相反，属于安全性脚本

version: 负责增强服务与版本扫描（Version Detection）功能的脚本

vuln: 负责检查目标机是否有常见的漏洞(Vulnerability)，如是否有 MS08_067