参考：
http://www.youknowi.xin/2018/05/%e4%ba%94%e6%9c%88%e6%8f%90%e5%89%8d%e6%80%bb%e7%bb%93%e7%af%87windowssqlmap-tamper-%e4%ba%86%e8%a7%a3/

给出一个常用命令

nmap -sV -Pn -v -sS -p0-65535 –script=vuln -iL 3.txt -oN nmap_results.txt

-Pn 不探测主机存活，直接扫描　–script=vuln 扫描常见的漏洞　-sV 探测服务版本　-v 实时打印扫描内容　-p 指定端口,默认是常用的 1000 个端口　可以添加-F 参数，是扫描默认的 100 个端口　-iL 指定 urls 文件　-oN　输出扫描后的文件　-sS 是采用 syn 扫描

## 1.nmap 信息收集整理：

P0 各种协议 PU udp 空包文 PE -PP -PM icmp
时序扫描 0-5 速度依次提升
sS 半开放 tcp syn 扫描
nmap -sU -p 80-500 192.168.5.5 被忽略的 udp 端口
sL
nmap 192.168.150.1/24 >1.txt
cat 1.txt |grep 192.168|cut -c 22-45
p0 6 tcp 1 icmp 2 igmp 17 udp
nmap -sP 192.168.2.2/24
无 ping 扫描 躲避防火墙
本地区域防火墙内 不会禁止 arp 请求
PA
nmap -sV -A 192.168.5.1

p ping 扫描
nmap -sP ip/24 扫描存活主机
nmap -p0 无 ping 扫描
nmap -PU -p 80-500 扫描 udp 开放端口但扫描不出 udp 端口
nmap -T0 时序扫描 0-5 速度依次提升
nmap -p
nmap 路由地址
nmap -sT 完成 tcp 三次握手
nmap -sF -sP
nmap sS 半开放 tcp syn 扫描 并没有完成 3 次握手
nmap sU p 80-500
nmap sI www.0day.co:80 空闲扫描 允许进行端口完全欺骗扫描 不行
nmap sV 协议服务的版本名

nmap sV --allports
nmap O 操作系统
nmap -D RND:11 ip 欺骗
nmap -sI www.0day.co:80 源地址欺骗 sI 主要用来源地址欺骗 也可以空闲扫描 不行
nmap --sources-port 53(DNS 端口) 源端口欺骗
namp --data-length 30(28)
nmap -sT -PN --spoof-mac 0
nmap -iL target.txt
nmap192.168.1.1/24-excludefilexxx.txt(xxx.txt 中的文件将会从扫描的主机中排除)
nmap-p80,21,23192.168.1.1