Nmap 参数解释

参数	说明
扫描目标	
域名，主机名称，ip 地址，网络号	如：scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
-iL <读入文件名>	从一个文件读取主机列表
-iR <主机数量>	选择随机目标
--exclude <主机 1[,主机 2][,主机 3]……>	排除的主机
--excludefile <排除列表文件名>	排除列表文件
主机发现	
-sL	列表扫描，并不会真正扫描，一般用来对扫描进行合理性检查。或者配合 dns 服务器对某些 ip 地址进行反向 DNS 查询。参考此处
-sn	Ping 扫描，不使用端口扫描
-Pn	强行扫描，视所有主机均在线，跳过主机发现步骤
-PS/PA/PU/PY [端口列表]	使用 TCP SYN/ACK, UDP or SCTP 来探测指定端口以此来发现主机，默认时 tcp、sctp 使作目标端口 80 来扫描，udp 使用 42125 来扫描，可后接品手动指定端口。
-PE/PP/PM	使用 icmp 回显，icmp 时间戳，icmp 网络掩码请求作为探测机制
-PO [协议列表]	使用 ip 协议 PING，默认使用的类型为 1，也就是 icmp 协议
-n/-R	永远不使用 dns 解析/一直使用 dns 解析，默认是偶尔解析
--dns-servers <serv1 [,serv2],…>	自定义 dns 服务器
--system-dns	使用操作系统的 dns 解析
--traceroute	对每个主机的路径都跟踪跳数
扫描技术	
-sS/sT/sA/sW/sM	TCP 的 SYN/Connect()/ACK/Window/Maimon 扫描
-sU	Udp 扫描
-sN/sF/sX	TCP Null, FIN, and Xmas 扫描
--scanflags <flags>	自定义 tcp 扫描的 flag，可供选择的有 ack,psh,rst,syn,fin
-sI <僵尸主机[:端口]>	空闲扫描
-sY/sZ	SCTP INIT/COOKIE-ECHO 扫描
-sO	Ip 协议扫描
-b <ftp 中继主机>	ftp 跳跃扫描

端口指定和扫描命令	
-p <端口范围>	扫描指定的端口，例如-p22；-p1-65535；-pU:53,111,137,T:21-25,80,139,8080,S:9
-F	快速扫描模式，比默认的扫描扫描更少的端口
-r	按顺序连续地扫描端口，不要随机扫描
--top-ports <数量>	扫描指定数量的熟知端口
--port-ratio <>	
服务/版本检测	
-sV	扫描开放端口的服务/版本信息
--version-intensity <等级>	设置扫描探测的强度，0 最低，9 最高
--version-light	限制为使用最可能的探测，等级相当于为 2
--version-all	尝试所有探测，等级相当于为 9
--version-trace	显示详细的扫描进度
脚本扫描	
-sC	使用默认的脚本扫描，相当于--script=default
--script=<Lua 脚本>	Lua 脚本表示是一个由逗号隔开的脚本目录，或脚本文件
--script-args=<n1=v1,[n2=v2,...]>	为脚本指定参数
--script-args-file=文件名	从文件引为脚本提供参数
--script-trace	显示所有发送和接收的数据
--script-updatedb	升级脚本数据库
--script-help=<Lua scripts>	显示脚本帮助
操作系统检测	
-O	使能操作系统检测
--osscan-limit	仅对把握较大的主机进行操作系统类型检测
--osscan-guess	更粗略地对操作系统类型进行探测
时间和性能	默认单位为秒，可以'ms' (milliseconds), 's' (seconds), 'm' (minutes), or 'h' (hours)
-T <0-5>	设置时间模板，值越大越快
--min-hostgroup/max-hostgroup <size>	并行扫描的主机组大小
--min-parallelism/max-parallelism <numprobes>	探测的并发量
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>	指定扫描的往返时间
--max-retries <tries>	最大重试次数
--host-timeout <time>	超时时间
--scan-delay/--max-scan-delay <time>	两个扫描之间的时延
--min-rate <number>	设置扫描发送的包的速度不小于设定值，单位是个每秒
--max-rate <number>	设置扫描发送的包的速度不大于设定值，单位是个每秒
防火墙/入侵检测系统的入侵和欺诈	
-f; --mtu <val>	对包进行分片，
-D <decoy1,decoy2[,ME],...>	对扫描进行伪装

-S <IP_Address>	伪装源 IP 地址
-e <iface>	使用指定的接口
-g/--source-port <portnum>	使用指定的源端口
--data-length <num>	在包后面附加随机数据
--ip-options <options>	使用指定的 ip 选项
--ttl <val>	设置 ip 的 ttl
--spoof-mac <mac address/prefix/vendor name>	伪装自己的 mac 地址
--badsum	指定错误的校验和
输出	
-oN/-oX/-oS/-oG <file>	输出分别为普通，xml，s|<rIpt kIddi3, and Grepable format
-oA <basename>	同时使用三种格式输出到同一个文件
-v	打印更详细的信息，可以多加几个 v 使输出更详细，如-vvvv
-d	设置调试级别，-dd 或更多的 d
--reason	显示端口处在特殊状态的原因
--open	仅显示打开的端口
--packet-trace	显示所有发送和接收的包
--iflist	打印主机的接口和路由，用于调试
--log-errors	记录错误
--append-output	附加而不是重写到指定文件
--resume <filename>	继续未完成的扫描
--stylesheet <path/URL>	转换输出为 html 格式
--webxml	更友好的 xml 格式
--no-stylesheet	不关联 xsl 或 x/xwl 样式
混合选项	
-6	使能 ipv6 扫描
-A	使能操作系统类型检测，服务检测，脚本扫描，并追踪路径
--datadir <dirname>	
--send-eth/--send-ip	
--privileged	
--unprivileged	
-V	显示版本号

黄龙舟

hlz_2599@163.com