Nmap 7.30 ( https://nmap.org )

使用方法: nmap [扫描类型(s)] [选项] {目标说明}

目标说明:

通过主机名称, IP 地址, 网段, 等等.

协议: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254

-iL <inputfilename>: 输入 主机或者网段

-iR <主机数>:随机选择目标

--exclude <主机1[,主机2][,主机3],...>: 排除的IP或者网段

--excludefile <exclude\_file>: 从文件中排除

主机发现:

-sL: List Scan - 简单的列出目标进行扫描

-sn: Ping Scan - 禁用端口扫描

-Pn: Treat all hosts as online -- 不使用主机发现

-PS/PA/PU/PY[portlist]: 通过TCP SYN/ACK, UDP or SCTP 等协议发现指定端口

-PE/PP/PM: 使用ICMP协议响应, 时间戳, 和子网掩码 请求 发现 探测

-PO[protocol list]: 使用ip协议

-n/-R: Never do DNS resolution/Always resolve [默认选项]

--dns-servers <serv1[,serv2],...>: 自动以DNS

--system-dns: 使用系统DNS

--traceroute: 跟踪每个主机的路径

扫描技术:

-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon 等协议扫描

-sU: UDP 扫描

-sN/sF/sX: 空的TCP, FIN, 和 Xmas 扫描

--scanflags <flags>:自定义tcp扫描

-sI <zombie host[:probeport]>: 空间扫描

-sY/sZ: SCTP初始化 或者 cookie-echo扫描

-sO: IP协议扫描

-b <FTP relay host>: FTP 反弹扫描

规范端口和扫描序列:

-p <port ranges>: 只扫描指定端口

使用规范: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9

--exclude-ports <port ranges>: 排除指定端口扫描

-F: 快速扫描- 扫描常用端口

-r: 连续端口扫描 - 不随机

--top-ports <number>: 扫描 <number> 常见的端口

--port-ratio <ratio>: Scan ports more common than <ratio>

服务和版本检测:

-sV: 探索开放的端口 以确定服务和版本号

--version-intensity <level>:设置从0-9所有的探针

--version-light:最有可能的漏洞探针(intensity 2)

--version-all: 尝试每一个漏洞探针 (intensity 9)

--version-trace: 显示详细的版本扫描活动 (调试)

扫描脚本的使用:

-sC: 默认脚本进行探测

--script=<Lua scripts>: <Lua scripts> 用 逗号分隔的列表, 脚本目录or 脚本类别

--script-args=<n1=v1,[n2=v2,...]>: 为脚本提供参数

--script-args-file=filename:在一个文件中提供NSE脚本（自定义脚本）

--script-trace: 显示所有发送和接收的数据

--script-updatedb: 更新脚本数据库

--script-help=<Lua scripts>: 显示脚本帮助

<Lua scripts> 是一个逗号分隔的脚本文件列表或脚本类.

操作系统识别:

-O: 使用操作系统探测

--osscan-limit: Limit OS detection to promising targets

--osscan-guess: Guess OS more aggressively

定时和性能:

用于定时任务 <时间> 在多少秒, 或者追加'毫秒' ,

'秒' , '分钟' , 或者 '小时'去设置 (e.g. 30m).

-T<0-5>: 设置定时模板 (更方便)

--min-hostgroup/max-hostgroup <size>: 并行扫描的最大值和最小值

--min-parallelism/max-parallelism <numprobes>: 并行扫描

--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: 指定扫描结束时间

--max-retries <tries>: Caps number of port scan probe retransmissions.

--host-timeout <time>: Give up on target after this long

--scan-delay/--max-scan-delay <time>: 调整每次扫描的延迟

--min-rate <number>: 发送的数据包不低于《数值》

--max-rate <number>: 发送的数据包不超过《数值》

防火墙/ IDS逃避和欺骗：

-f; --mtu <val>: 碎片包 (可以选择 w/given MTU)

-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys

-S <IP\_Address>: 源地址欺骗

-e <iface>: 使用指定的接口

-g/--source-port <portnum>:使用给定的端口号

--proxies <url1,[url2],...>: Relay 通过使用 HTTP/SOCKS4 代理

--data <hex string>:附加一个自定义的有效载荷发送数据包

--data-string <string>: 添加一个自定义的ASCII字符串发送的数据包

--data-length <num>: 附加随机数据发送数据包

--ip-options <options>: 用指定的IP选项发送数据包

--ttl <val>: 设置ip到达目标的时间

--spoof-mac <mac address/prefix/vendor name>:欺骗本地MAC地址

--badsum:发送用来效验的伪造数据包 TCP/UDP/SCTP

输出:

-oN/-oX/-oS/-oG <file>:输出正常的扫描, XML格式, s|<rIpt kIddi3,

和 Grepable 格式, respectively,或者指定的文件名

-oA <basename>: 一次输出三种主要格式

-v: 增加详细程度 (使用 -vv 显示更详细)

-d: 提高测试的详细程度 (使用 -dd参数更详细)

--reason: 显示端口处于某个特定状态的原因

--open: 只显示开放的端口

--packet-trace: 显示发送和接收的所有数据包

--iflist:打印主机接口和路由

--append-output: 附加到指定的输出文件

--resume <filename>: 回复终止的扫描

--stylesheet <path/URL>: XSL样式表转换XML输出HTML

--webxml: 从Nmap参考样式。或者更便携的XML

--no-stylesheet: Prevent associating of XSL stylesheet w/XML output

杂项:

-6: 启用ipv6扫描

-A: 使操作系统版本检测，检测，脚本扫描和跟踪

--datadir <dirname>: 指定自定义可以使用的数据文件位置

--send-eth/--send-ip:发送使用原始以太网帧或IP数据包

--privileged: 假设用户是最高权限

--unprivileged: 假设用户缺乏原始套接字特权

-V: 打印当前版本

-h: 显示英文帮助文档.

举例:

nmap -v -A scanme.nmap.org

nmap -v -sn 192.168.0.0/16 10.0.0.0/8

nmap -v -iR 10000 -Pn -p 80

查看帮助网页 (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES