nmap 扫描端口

主机发现

iR	随机选择目标
-iL	从文件中加载IP地址
-sL	简单的扫描目标
-sn	Ping扫描-禁用端口扫描
-Pn	将所有主机视为在在线，跳过主机发现
-PS[portlist]	（TCP SYN ping） 需要root权限
-PA[portlist]	（TCP ACK ping）
-PU[portlist]	（UDP ping）
-PY [portlist]	（SCTP ping）
-PE/PP/PM	ICMP回显，时间戳和网络掩码请求探测
-PO[协议列表]	IP协议Ping
-n/-R	从不执行DNS解析/始终解析[默认：有时]
--dns-servers	指定自定义DNS服务器
--system-dns	使用OS的dns服务器
--traceroute	跟踪到每个主机的跃点路径

扫描技术

-sS	使用TCP的SYN进行扫描
-sT	使用TCP进行扫描
-sA	使用TCP的ACK进行扫描
-sU	UDP扫描
-sI	Idle扫描

-sF FIN扫描

-b<FTP中继主机> FTP反弹扫描

端口规格和扫描顺序

-p 扫描指定端口

--exclude-ports 从扫描中排除指定端口

-f 快速模式-扫描比默认扫描更少的端口

-r 连续扫描端口-不随机化

--top-ports 扫描<number>最常用的端口

服务/版本探测

-sV 探测服务/版本信息

--version-intensity 设置版本扫描强度（0-9）

--version-all 尝试每个强度探测

--version-trace 显示详细的版本扫描活动（用于调试）

脚本扫描

-sC 等效于 --script=defult

--script = <lua scripts>,<lua scripts> 以逗号分隔的目录，脚本文件或脚本类别

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

--script-args-file=文件名 从文件名中加载脚本参数

--script-trace 显示发送和接受的所有数据

--script-updatedb 更新脚本数据库

--script-help=<lua scripts> 显示有关脚本的帮助

操作系统检测

-o 启用os检测

--osscan-limit 将os检测限制为可能的目标

--osscan-guess 推测操作系统检测结果

时间和性能

--host-timeout 设置超时时间

--scan-delay 设置探测之间的时间间隔

-T <0-5> 设置时间模板,值越小，IDS报警几率越低

防火墙/IDS规避和欺骗

-f 报文分段

-s 欺骗源地址

-g 使用指定的本机端口

--proxies <url,port> 使用HTTP/SOCK4代理

-data<hex string> 想发送的数据包中追加自定义的负载

--data-string 将自定义的ACSII字符串附加到发送数据包中

--data-length 发送数据包时，附加随机数据

--spoof-mac MAC地址欺骗

--badsum 发送带有虚假TCP/UNP/STCP校验和的数据包

输出

-oN 标准输出

-oX XML输出

-oS script jlddi3

-oG grepable

-oA 同时输出三种主要格式

-v 信息详细级别

-d 调试级别

--packet-trace 跟踪发送和接收的报文

--reason 显示端口处于特殊状态的原因

--open 仅显示开放的端口

杂项

-6 启动Ipv6扫描

-A 启动Os检测，版本检测，脚本扫描和traceroute

-V 显示版本号

-h	帮助信息

arping发现目标mac地址

fping探测主机存活

msfadmin