|  |  |
| --- | --- |
| Nmap主机发现： | |
| -sP \*  -P0 \*  -PS \*  -PA \*  -PU \*  -PE/PM/PP \*  -PR \*  -n \*  -R \*  –system-dns \*  -sL \*  -6 \*  –traceroute \*  -PY \* | Ping扫描 \*  无Ping扫描 \*  TCP SYN Ping扫描 \*  TCP ACK Ping扫描 \*  UDP ping扫描  ICMP Ping Types扫描  ARP Ping扫描  禁止DNS反向解析 \*  反向解析域名 \*  使用系统域名解析器  列表扫描 \*  扫描IPv6地址  路由跟踪  SCTP INIT Ping扫描 |

**Ping 扫描**:

nmap -sP www.baidu.com

nmap -sP 192.168.1.0

无ping扫描:常用于防火墙禁止ping的情况，可穿透防火墙

nmap -P0 192.168.1.0

TCP SYN Ping扫描(默认80号端口,nmap通过SYN/ACK和RST的响应来判断,防火墙可能会丢弃RST包)

nmap -PS -v www.baidu.com

指定端口范围

nmap -PS80,100-200 -v www.baidu.com

TCP ACK Ping扫描(很多防火墙会封锁SYN报文,此时可以使用TCP ACK ping扫描)

nmap -PA www.baidu.com

ARP Ping扫描(一般用于扫描局域网)

nmap -PR 192.168.10.0

列表扫描

nmap -sL 192.168.10.1/24

禁止反向域名解析(不对目标ip地址作反向域名解析,单纯扫描一段ip时，使用该选项可以减少扫描时间)

nmap -n -sL 192.168.10.1/24

路由跟踪(需要root权限)

nmap --traceroute -sP 192.168.10.1

SCTP INIT Ping扫描(流控制传输协议,向目标发送INIT包,需要root权限)

nmap -PY -v 192.168.10.1

**Nmap的6种端口状态:**

\* Open

\* Closed

\* Filtered:可能被过滤，可能网络阻塞

\* Unfiltered:可以访问，但未知端口处于开放还是关闭状态

\* Open|Filtered

\* Closed|Filtered:不能确定端口事关闭还说被过滤

-T \* 时序选项

-p|-F|-r \* 常用扫描方式

-sS \* TCP SYN扫描:(需要root权限)

-sT \* TCP连接扫描:完整三次握手，最基础最稳定的扫描方式

-sU \* UDP扫描(速度非常慢，一般用-p指定端口范围以节约时间)

-sN/sF/sX \* 隐蔽扫描

-sA \* TCP ACK扫描

-sW \* TCP窗口扫描

-sM \* TCP Maimon扫描

–scanflags \* 自定义TCP扫描

-sI \* 空闲扫描

-sO \* IP协议扫描

-b \* FTP Bounce扫描

**常用扫描方式**：

**指定端口扫描：**

nmap -p 80 192.168.10.1

nmap -p 80-1000 192.168.10.1

**TCP SYN扫描**：又称为半开放扫描，常见扫描方式，扫描速度较快

由于未进行TCP连接，比较隐蔽，很难背防火墙或管理员发现

nmap -sS 172.20.62.150(需要root权限)

**隐蔽扫描**:

-sN是Null扫描

-sF是Fin扫描(发送FIN包)

-sX是Xmas扫描(将数据包的FIN／PSH／URG都标记为1)

**Nmap指纹识别与探测**

-sV \* 版本探测

nmap -sV -A www.baidu.com–allports \* 全端口版本探测

–version-intensity \* 设置扫描强度

nmap -sV –version-intensity 1 www.baidu.com

–version-light \* 轻量级扫描

nmap -sV –version-light www.baidu.com

–version-all \* 重量级扫描

–version-trace \* 获取详细版本信息

-sR \* RPC扫描

-O \* 启用操作系统探测 \*

–osscan-limit \* 对指定的目标进行系统探测

–osscan-guess/–fuzzy \* 推测系统识别

**防火墙／IDS逃逸**

入侵检测系统(Intrusion Detection Systems, IDS)

-f \* 报文分段

将TCP头分段在几个包中，使得包过滤器、IDS以及其他工具的检测更加困难。例:某些主机会禁止相应ICMP请求，使用报文分段的方法可以逃避目标防火墙的规则，使用该选项时需小心，处置不当可能会出现某些错误

nmap -f -v 192.168.10.1

–mtu \* 指定偏移大小

用于设置TCP／IP协议传输数据报时的最大传输单元，注意：偏移量必须时8的倍数

nmap –mtu 16 192.168.10.1

-D \* IP欺骗

11个随机的ip地址向目标主机发送SYN包

RND：随机生成地址

nmap -D RND:11 192.168.10.1

使用4个指定的ip地址对目标进行扫描,ME为自己的真实ip

nmap -D 192.168.0.1,192.168.0.2,192.168.0.254,ME 192.168.10.1

-sI \* 源地址欺骗

–source-port \* 源端口欺骗(也可使用-g)

nmap –source-port 53 192.168.10.1 //指定53号端口进行扫描

–spoof-mac \* MAC地址欺骗

参数:

0:随机生成一个mac地址

MAC Address:手动指定一个Mac地址

Vendor Name:从指定厂商生产一个mac地址

nmap -sT -PN –spoof-mac 0 192.168.10.1

**信息搜集**

–script ip-geolocation-\* \* ip信息搜集(root)

nmap –script ip-geolocation-\* www.baidu.com

如果目标域名使用了CDN，则获取的ip等信息并不是目标域名的真实信息

dns-brute \* dns信息搜集

dns使用tcp和udp的53号端口

每一级域名长度限制是63个字符，域名总长度不能超过253个字符。

dns-brute \* 列举dns服务器的主机名

对baidu.com子域名进行枚举

nmap –script dns-brute –script-args dns-brute.domain=baidu.com

membase-http-info \* 检索系统信息

nmap -p 445 192.168.10.1 –script membase-http-info

了解系统详细信息

http-headers/http-sitemap-generator \* http信息搜集

对http版本进行探测

nmap -sV -p 80 www.baidu.com

http头信息探测

nmap -p 80 –script=http-headers www.baidu.com

http目录结构探测

nmap -p 80 –script=http-sitemap-generator www.baidu.com

**nmap快捷命令**

nmap --send-eth 192.168.10.1//发送以太网数据包

nmap --send-ip 192.168.10.1//网络层发送

nmap --privileged 192.168.10.1//假定拥有所有权

nmap -d 1 192.168.10.1//设置调试级别

nmap -iflist 192.168.10.1//列举接口和路由:（多用于调试路由）

nmap -e en0 192.168.10.1//指定网络接口：指定从en0发送数据

nmap --script=firewalk --traceroute 192.168.10.1//探测防火墙

**nmap保存和输出**

-oN \* 标准保存

nmap -F -oN test1.txt 192.168.10.1

-oX \* XML保存

nmap -F -oX test1.xml 192.168.10.1

-oA \* 保存到所有格式

nmap -F -oA testA 192.168.10.1