Cheatography

nmap-zh Cheat Sheet

by fkbug via cheatography.com/84111/cs/19877/

扫描目标

参数	描述	示例
	扫描多个IP	nmap 192.168.1.1
	扫描特定IP	nmap 192.168.1.1 192.168.2.1
	扫描范围	nmap 192.168.1.1-254
	扫描 CIDR 表示范围	nmap 192.168.1.0/24
	扫描域名	nmap scanme.nmap.org
-iL	从文件中导入目标	nmap -iL targets.txt
-iR	随机选择目标	nmap -iR 100
--exclude	排除列出的目标	nmap --exclude 192.168.1.1
--excludefile	排除文件中的目标	nmap --excludefile notargets.txt

端口设置

参数	描述	示例
-p	端口扫描 端口x	nmap -p 21 192.168.1.1
-p	端口扫描 端口范围	nmap -p 21-100 192.168.1.1
-p	端口扫描 多个 TCP及UDP端口	nmap -p U:53, T:21-25,80 192.168.1.1
-p-	端口扫描 所有端口	nmap -p- 192.168.1.1
-F	端口扫描 快速模式(仅扫描 TOP100 端口)	nmap -F 192.168.1.1
--top-ports number	端口扫描 扫描开放概率最高的 number 个端口	nmap --top-ports 2000 192.16-8.1.1
-r	端口扫描 顺序扫描(nmap 默认会打乱端口的扫描顺序以防止防火墙检测，开启该参数后将变为顺序扫描	nmap -p- -r 192.168.1.1
--port-ratio <ratio>	扫描指定频率以上的端口(以端口开放概率作为参数，为0~1 之间)	nmap -port-ratio 0.9 192.168.1.1

主机发现

参数	描述	示例
-sL	List scan(没有扫描，仅列出目标)	nmap -sL 192.168.1-3
-sn	Ping scan(只进行主机发现，禁用端口扫描) 在早期版本中，也写成 -sP	nmap -sn 192.168.1.1/24
-Pn	Port scan(跳过主机发现，将所有主机视为已开启，直接端口扫描)	nmap -Pn 192.168.1-5
-PS [portlist]	端口x 上的 TCP SYN主机发现，默认端口80	nmap -PS22-25,80 192.168.1.1-5
-PA [portlist]	端口x 上的 TCP ACK主机发现，默认端口 80	nmap -PA22-25,80 192.168.1.1-5

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com

主机发现 (cont)

-PU [portlist]	端口x 上的 UDP 主机发现，默认端口为 40125	nmap -PU53 192.168.1.1-5
-PY [portlist]	端口x 上的 SCTP 主机发现	nmap -PY22-25,80 192.168.1.1-5
-PE	使用 ICMP echo 请求包发现主机	nmap -PE 192.168.1.1
-PP	使用 ICMP timestamp 请求包发现主机	nmap -PP 192.168.1.1
-PM	使用 ICMP netmask 请求包发现主机	nmap -PM 192.168.1.1
-PO	使用 IP 协议包探测目标主机是否开启	nmap -PO 192.168.1.1
-PR	本地网络上的 ARP 发现	nmap -PR 192.168.1.1/24
-n	表示不进行 dns 解析(反向 dns 解析会很明显的减慢 nmap 的扫描时间，在扫描大量主机时如果不关心其 dns 信息可以使用此参数加快扫描速度)	nmap -n 192.168.1.1
-R	表示总是进行 dns 解析	nmap -R 192.168.1.1
--system-dns	指定使用主机系统自带的的 dns 解析器，而不是 nmap 内部的方法	nmap --system-dns 192.168.1.1
--dns-servers <serv1[,serv2],..>	手动指定dns 服务器	nmap --dns-servers dnsIP1 dnsIP2 192.168.1.1
--traceroute	跟踪主机的路径（适用于除连接扫描 -sT 和空闲扫描 -sI 之外的所有扫描类型)	nmap --traceroute 192.168.1.1
--resolve-all	扫描每个已解析的地址(如果主机目标解析为多个地址则扫描所有地址，默认行为是仅扫描第一个已解析的地址)	nmap --resolve-all baidu.com

扫描方式

参数	描述	示例
-sS	**TCP SYN 端口扫描(默认)**	nmap -sS 192.168.1.1
-sT	TCP 连接端口扫描(默认无 root 权限)	nmap -sT 192.168.1.1
-sA	TCP ACK 端口扫描	nmap -sA 192.168.1.1
-sW	TCP 窗口 端口扫描	nmap -sW 192.168.1.1
-sM	TCP Maimon 端口扫描	nmap -sM 192.168.1.1
-sU	UDP 端口扫描	nmap -sU 192.168.1.1
-sN	TCP Null 秘密扫描	nmap -sN 192.168.1.1
-sF	TCP FIN 秘密扫描	nmap -sF 192.168.1.1
-sX	TCP Xmas 秘密扫描	nmap -sX 192.168.1.1
--scanflags <flags>	TCP 包标志位 定制扫描	nmap --scanflags URGFIN 192.168.1.1

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com

扫描方式 (cont)

-sI	Idle 扫描(没有报文是从真实IP发送到目标的）需要找到合适的 Zombie 主机)	nmap -Pn -p- -sI Zombie.com target.com
-sY	SCTP INIT 扫描(SCTP 可以看作是 TCP 协议的改进）这种扫描向目标发送 INIT 包来判断目标是否存活	nmap -sY 192.168.1.1
-sZ	SCTP COOKIE_ECHO 扫描	nmap -sZ 192.168.1.1
-sO	IP 协议扫描(确定目标支持哪些 IP 协议） TCP、ICMP、IGMP等等	nmap -sO 192.168.1.1
-b <FTP relay host>	FTP 反弹扫描(连接到防火墙后面的一台FTP服务器做代理，接着进行端口扫描）	nmap -Pn -b ftp.microsfot.com google.com

版本侦测

参数	描述	示例
-sV	尝试确定在端口上运行的服务的版本	nmap -sV 192.168.1.1
--version-intensity <level>	指定版本侦测的强度(0-9),默认为7，数值越高，探测出的服务越准确，但运行时间也越长	nmap -sV --version-intensity 8 192.168.1.1
--version-light	指定使用轻量级侦测方式(intensity=2)	nmap -sV --version-light 192.168.1.1
--version-all	指定使用所有的版本侦测(intensity=9)	nmap -sV --version-all 192.168.1.1
--version-trace	显示出详细的版本侦测过程信息	nmap -sV --version-trace 192.168.1.1

系统侦测

参数	描述	示例
-O	使用 TCP/IP 指纹进行远程系统检测	nmap -O 192.168.1.1
-O --osscan-limit	如果一个打开或关闭的 TCP 端口都没找到，则不进行系统探测尝试	nmap -O --oscan-limit 192.168.1.1
-O --osscan-guess	使 nmap 更积极地猜测目标系统信息	nmap -O --osscan-guess 192.168.1.1
-O --max-os-tries	设置针对目标的 OS 检测尝试的最大次数	nmap -O --max-os-tries 1
-A	启用操作系统探测，版本检测，脚本扫描以及路由跟踪	nmap -A 192.168.1.1

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com

时间性能

参数	描述	示例
-T0	偏执的	nmap -T0 192.168.1.1
-T1	悄悄的	nmap -T1 192.168.1.1
-T2	礼貌的	nmap -T2 192.168.1.1
-T3	默认的	nmap -T3 192.168.1.1
-T4	激烈的	nmap -T4 192.168.1.1
-T5	疯狂的	nmap -T5 192.168.1.1
--host-timeout <time>	time 时长后仍未扫描完毕则放弃	nmap -host-timeout 30m 192.168.1.1
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>	指定探测包往返时间	nmap --min-rtt-timeout 2s 192.168.1.1
--scan-delay/--max-scan-delay <time>	指定探测包的延迟	nmap --scan-delay 3min 192.168.1.1
--max-retries <tries>	指定端口扫描探测包重新传输的最大数量	nmap --max-retries 3 192.168.1.1
--min-rate <number>	指定发送的数据包不低于每秒 number 个	nmap --min-rate 100 192.168.1.1
--max-rate <number>	指定发送的数据包不超过每秒 number 个	nmap --max-rate 100 192.168.1.1

-T 表示 nmap 扫描过程中使用的速度，级别越高，扫描速度越快，但也越容易被防火墙或 IDS 检测并屏蔽掉，在通信状况良好的情况下推荐使用 T4。nmap 一般默认为 T3，而 T2 基本就是 T3 的百倍时间了，所以 T3 以下都是为了规避防火墙或 IDS 的检测，速度越慢越不容易被检测到。

结果输出

参数	描述	示例
-oN	正常输出	nmap 192.168.1.1 -oN normal.file
-oX	XML 格式输出	nmap 192.168.1.1 -oX xml.file
-oG	可过滤的输出	nmap 192.168.1.1 -oG grep.file
-oA	一次输出三种主要格式	nmap 192.168.1.1 -oA results
-oG -	同时输出到屏幕，-oN -, -oX - 同理	nmap 192.168.1.1 -oG -
--append	将扫描结果附加到上一个扫描文件	nmap 192.168.1.1 -oN file.file --append-output
-v	增加扫描过程详细程度(-vv 可以增加扫描过程的详细程度)	nmap -v 192.168.1.1
-d	增加扫描过程中的调试信息(-dd 则增加更多的调试信息)	nmap -d 192.168.1.1
--reason	显示端口处于特定状态的原因等信息(等价于 -vv)	nmap --reason 192.168.1.1
--open	只显示为开启状态的端口的信息	nmap --open 192.168.1.1
--packet-trace	显示扫描过程中所有发送和接收的包	nmap -T4 --packet-trace 192.168.1.1

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com

结果输出 (cont)

--iflist	显示主机接口和路由信息	nmap --iflist
--resume	恢复扫描	nmap --resume result.file

常用输出示例

功能	命令
扫描并过滤出 web 服务器：	nmap -p80 -sV -oG - --open 192.168.1.1/24 | grep open
生成存活主机列表：	nmap -iR 10 -n -oX out.xml | grep "Nmap" | cut -d " " -f5 >> live-host.txt
附加新发现的存活主机：	nmap -iR 10 -n -oX out2.xml | grep "Nmap" | cut -d " " -f5 >> live-host.txt
比较 nmap 的扫描结果:	ndiff scan.xml scan2.xml
把 xml 的输出结果转为 html	xsltproc nmap.xml -o nmap.html
按端口频率降序排列扫描结果	grep "open" results.nmap | sed -r 's / + / / g' |sort |uniq -c |sort -rn | less

grep、sed、sort、less 主要为 bash 命令，所以有些输出组合可能 windows 下无法使用

杂项

参数	描述	示例
-6	开启 IPv6 扫描	nmap -6 192.168.1.1
-A	开启 系统探测、版本探测、默认脚本扫描、traceroute	nmap -A 192.168.1.1
--data-dir <dirname>	指定自定义 nmap 数据文件目录位置	nmap --data-dir /root/ 192.168.1.1
--send-eth/--send-ip	使用原始以太帧或 IP 报文	nmap --send-eth 192.168.1.1
--privileged	假定用户为特权账户	nmap --privileged 192.168.1.1
--unprivileged	假定用户未获得所有权限	nmap --unprivileged 192.168.1.1
-V	打印 nmap 版本信息	nmap -V
-h/--help	打印 nmap 帮助文档	nmap -h

防火墙/IDS 绕过

参数	描述	示例
-f		

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com