nmap 常用扫描参数及说明

1. -sT TCP connect()扫描，这种方式会在目标主机的日志中记录大批连接请求和错误信息 。
2. -sS 半开扫描，很少有系统能够把它记入系统日志。不过，需要 root 权限。
3. -sF 秘密 FIN 数据包扫描，Xmas Tree、Null 扫描模式。
4. -sP ping 扫描，Nmap 在扫描端口时，默认会使用 ping 扫描，只有主机存活，Nmap 才会继续扫描。
5. -sU UDP 扫描，但 UDP 扫描是不可靠的。
6. -sA 这项高级的扫描方法通常用来穿过防火墙的规则集。
7. -sV 探测端口服务版本。
8. -PO 扫描之前不需要用 ping 命令，有些防火墙禁止用 ping 命令。可以使用此选项进行扫描
9. -v 显示扫描过程。
10. -h 帮助选项，是最清楚的帮助文档。
11. -p 指定端口，如"1~65536、1433、135、22、80"等。
12. -O 启用远程操作系统检测，存在误报。
13. -A 全面系统检测、启用脚本检测、扫描等。
14. -oN/-oX/-oG 将报告写入文件，分别是正常、XML、grepable 三种格式。
15. -T4 针对 TCP 端口禁止动态扫描延迟超过 10ms
16. -iL 读取主机列表，例如，“iL C:\ip.txt”。

扫描类型

-sT

TCP connect()扫描：这是最基本的 TCP 扫描方式。connect()是一种系统调用，由操作系统提供，用来打开一个连接。如果目标端口有程序监听， connect()就会成功返回，否则这个端口是不可达的。这项技术最大的优点是，你勿需 root 权限。任何 UNIX 用户都可以自由使用这个系统调用。这种扫描很容易被检测到，在目标主机的日志中会记录大批的连接请求以及错误信息。

-sS

TCP 同步扫描(TCP SYN)：因为不必全部打开一个 TCP 连接，所以这项技术通常称为半开扫描(half-open)。你可以发出一个 TCP 同步包(SYN)，然后等待回应。如果对方返回 SYN|ACK(响应)包就表示目标端口正在监听；如果返回 RST 数据包，就表示目标端口没有监听程序；如果收到一个 SYN|ACK 包，源主机就会马上发出一个 RST(复位)数据包断开和目标主机的连接，这实际上有我们的操作系统内核自动完成的。这项技术最大的好处是，很少有系统能够把这记入系统日志。不过，你需要 root 权限来定制 SYN 数据包。

-sF -sX -sN

秘密 FIN 数据包扫描、圣诞树(Xmas Tree)、空(Null)扫描模式：即使 SYN 扫描都无法确定的情况下使用。一些防火墙和包过滤软件能够对发送到被限制端口的 SYN 数据包进行监视，而且有些程序比如 synlogger 和 courtney 能够检测那些扫描。这些高级的扫描方式可以逃过这些干扰。这些扫描方式的理论依据是：关闭的端口需要对你的探测包回应 RST 包，而打开的端口必需忽略有问题的包(参考 RFC 793 第 64 页)。FIN 扫描使用暴露的 FIN 数据包来探测，而圣诞树扫描打开数据包的 FIN、URG 和 PUSH 标志。不幸的是，微软决定完全忽略这个标准，另起炉灶。所以这种扫描方式对 Windows95/NT 无效。不过，从另外的角度讲，可以使用这种方式来分别两种不同的平台。如果使用这种扫描方式可以发现打开的端口，你就可以确定目标主机运行的不是 Windows 系统。如果使用-sF、-sX 或者-sN 扫描显示所有的端口都是关闭的，而使用 SYN 扫描显示有打开的端口，你可以确定目标主机可能运行的是 Windwos 系统。现在这种方式没有什么太大的用处，因为 nmap 有内嵌的操作系统检测功能。还有其它几个系统使用和 windows 同样的处理方式，包括 Cisco、BSDI、HP/UX、MYS、IRIX。在应该抛弃数据包时，以上这些系统都会从打开的端口发出复位数据包。

-sP

ping 扫描：有时你只是想知道此时网络上哪些主机正在运行。通过向你指定的网络内的每个 IP 地址发送 ICMP echo 请求数据包，nmap 就可以完成这项任务。如果主机正在运行就会作出响应。不幸的是，一些站点例如：microsoft.com 阻塞 ICMP echo 请求数据包。然而，在默认的情况下 nmap 也能够向 80 端口发送 TCP ack 包，如果你收到一个 RST 包，就表示主机正在运行。nmap 使用的第三种技术是：发送一个 SYN 包，然后等待一个 RST 或者 SYN/ACK 包。对于非 root 用户，nmap 使用 connect()方法。在默认的情况下(root 用户)，nmap 并行使用 ICMP 和 ACK 技术。注意，nmap 在任何情况下都会进行 ping 扫描，只有目标主机处于运行状态，才会进行后续的扫描。如果你只是想知道目标主机是否运行，而不想进行其它扫描，才会用到这个选项。

-sU
UDP 扫描：如果你想知道在某台主机上提供哪些 UDP(用户数据报协议,RFC768)服务，可以使用这种扫描方法。nmap 首先向目标主机的每个端口发出一个 0 字节的 UDP 包，如果我们收到端口不可达的 ICMP 消息，端口就是关闭的，否则我们就假设它是打开的。

-sA
ACK 扫描：这项高级的扫描方法通常用来穿过防火墙的规则集。通常情况下，这有助于确定一个防火墙是功能比较完善的或者是一个简单的包过滤程序，只是阻塞进入的 SYN 包。
这种扫描是向特定的端口发送 ACK 包(使用随机的应答/序列号)。如果返回一个 RST 包，这个端口就标记为 unfiltered 状态。如果什么都没有返回，或者返回一个不可达 ICMP 消息，这个端口就归入 filtered 类。注意，nmap 通常不输出 unfiltered 的端口，所以在输出中通常不显示所有被探测的端口。显然，这种扫描方式不能找出处于打开状态的端口。

-sW
对滑动窗口的扫描：这项高级扫描技术非常类似于 ACK 扫描，除了它有时可以检测到处于打开状态的端口，因为滑动窗口的大小是不规则的，有些操作系统可以报告其大小。这些系统至少包括：某些版本的 AIX、Amiga、BeOS、BSDI、Cray、Tru64 UNIX、DG/UX、OpenVMS、Digital UNIX、OpenBSD、OpenStep、QNX、Rhapsody、SunOS 4.x、Ultrix、VAX、VXWORKS。从 nmap-hackers 邮件 3 列表的文档中可以得到完整的列表。

-sR
RPC 扫描。这种方法和 nmap 的其它不同的端口扫描方法结合使用。选择所有处于打开状态的端口向它们发出 SunRPC 程序的 NULL 命令，以确定它们是否是 RPC 端口，如果是，就确定是哪种软件及其版本号。因此你能够获得防火墙的一些信息。诱饵扫描现在还不能和 RPC 扫描结合使用。

-b
FTP 反弹攻击(bounce attack):FTP 协议(RFC 959)有一个很有意思的特征，它支持代理 FTP 连接。也就是说，我能够从 evil.com 连接到 FTP 服务器 target.com，并且可以要求这台 FTP 服务器为自己发送 Internet 上任何地方的文件！1985 年，RFC959 完成时，这个特征就能很好地工作了。语法格式为：-b username:password@server:port

通用选项
这些内容不是必需的，但是很有用。

-P0
在扫描之前，不必 ping 主机。有些网络的防火墙不允许 ICMP echo 请求穿过，使用这个选项可以对这些网络进行扫描。microsoft.com 就是一个例子，因此在扫描这个站点时，你应该一直使用-P0 或者-PT 80 选项。

-PT
扫描之前，使用 TCP ping 确定哪些主机正在运行。nmap 不是通过发送 ICMP echo 请求包然后等待响应来实现这种功能，而是向目标网络(或者单一主机)发出 TCP ACK 包然后等待回应。如果主机正在运行就会返回 RST 包。只有在目标网络/主机阻塞了 ping 包，而仍旧允许你对其进行扫描时，这个选项才有效。对于非 root 用户，我们使用

connect()系统调用来实现这项功能。使用-PT <端口号>来设定目标端口。默认的端口号是 80，因为这个端口通常不会被过滤。

-PS
对于 root 用户，这个选项让 nmap 使用 SYN 包而不是 ACK 包来对目标主机进行扫描。如果主机正在运行就返回一个 RST 包(或者一个 SYN/ACK 包)。

-PI
设置这个选项，让 nmap 使用真正的 ping(ICMP echo 请求)来扫描目标主机是否正在运行。使用这个选项让 nmap 发现正在运行的主机的同时，nmap 也会对你的直接子网广播地址进行观察。直接子网广播地址一些外部可达的 IP 地址，把外部的包转换为一个内向的 IP 广播包，向一个计算机子网发送。这些 IP 广播包应该删除，因为会造成拒绝服务攻击(例如 smurf)。

-PB
这是默认的 ping 扫描选项。它使用 ACK(-PT)和 ICMP(-PI)两种扫描类型并行扫描。如果防火墙能够过滤其中一种包，使用这种方法，你就能够穿过防火墙。

-O
这个选项激活对 TCP/IP 指纹特征(fingerprinting)的扫描，获得远程主机的标志。换句话说，nmap 使用一些技术检测目标主机操作系统网络协议栈的特征。nmap 使用这些信息建立远程主机的指纹特征，把它和已知的操作系统指纹特征数据库做比较，就可以知道目标主机操作系统的类型。

-I
这个选项打开 nmap 的反向标志扫描功能。Dave Goldsmith 1996 年向 bugtap 发出的邮件注意到这个协议，ident 协议(rfc 1413)允许使用 TCP 连接给出任何进程拥有者的用户名，即使这个进程并没有初始化连接。例如，你可以连接到 HTTP 端口，接着使用 identd 确定这个服务器是否由 root 用户运行。这种扫描只能在同目标端口建立完全的 TCP 连接时(例如：-sT 扫描选项)才能成功。使用-I 选项是，远程主机的 identd 精灵进程就会查询在每个打开的端口上监听的进程的拥有者。显然，如果远程主机没有运行 identd 程序，这种扫描方法无效。

-f
这个选项使 nmap 使用碎片 IP 数据包发送 SYN、FIN、XMAS、NULL。使用碎片数据包增加包过滤、入侵检测系统的难度，使其无法知道你的企图。不过，要慎重使用这个选项！有些程序在处理这些碎片包时会有麻烦，我最喜欢的嗅探器在接受到碎片包的头 36 个字节时，就会发生 segmentation faulted。因此，在 nmap 中使用了 24 个字节的碎片数据包。虽然包过滤器和防火墙不能防这种方法，但是有很多网络出于性能上的考虑，禁止数据包的分片。
　　注意这个选项不能在所有的平台上使用。它在 Linux、FreeBSD、OpenBSD 以及其它一些 UNIX 系统能够很好工作。

-v
冗余模式。强烈推荐使用这个选项，它会给出扫描过程中的详细信息。使用这个选项，你可以得到事半功倍的效果。使用-d 选项可以得到更加详细的信息。

-h
快速参考选项。

-oN
把扫描结果重定向到一个可读的文件 logfilename 中。

-oM

把扫描结果重定向到 logfilename 文件中，这个文件使用主机可以解析的语法。你可以使用-oM -来代替 logfilename，这样输出就被重定向到标准输出 stdout。在这种情况下，正常的输出将被覆盖，错误信息茬苒可以输出到标准错误 stderr。要注意，如果同时使用了-v 选项，在屏幕上会打印出其它的信息。

-oS
把扫描结果重定向到一个文件 logfilename 中，这个文件使用一种"黑客方言"的语法形式。同样，使用-oS -就会把结果重定向到标准输出上。

-resume
某个网络扫描可能由于 control-C 或者网络损失等原因被中断，使用这个选项可以使扫描接着以前的扫描进行。logfilename 是被取消扫描的日志文件，它必须是可读形式或者机器可以解析的形式。而且接着进行的扫描不能增加新的选项，只能使用与被中断的扫描相同的选项。nmap 会接着日志文件中的最后一次成功扫描进行新的扫描。

-iL
从 inputfilename 文件中读取扫描的目标。在这个文件中要有一个主机或者网络的列表，由空格键、制表键或者回车键作为分割符。如果使用-iL -，nmap 就会从标准输入 stdin 读取主机名字。你可以从指定目标一节得到更加详细的信息。

-iR
让 nmap 自己随机挑选主机进行扫描。

-p
这个选项让你选择要进行扫描的端口号的范围。例如，-p 23 表示：只扫描目标主机的 23 号端口。-p 20-30,139,60000-表示：扫描 20 到 30 号端口，139 号端口以及所有大于 60000 的端口。在默认情况下，nmap 扫描从 1 到 1024 号以及 nmap-services 文件(如果使用 RPM 软件包，一般在/usr/share/nmap/目录中)中定义的端口列表。

-F
快速扫描模式，只扫描在 nmap-services 文件中列出的端口。显然比扫描所有 65535 个端口要快。

-D
使用-D 选项可以指定多个 ip 地址，或者使用 RND 随机生成多个地址；使用这个命令可可能会让目标主机管理员认为该扫描使用的是诱饵主机进行扫描的，而不是真实的扫描地址，因此会忽略这次扫描，从而，我们可以可以使用自己真实的 ip 地址进行扫描，以达到欺骗目标主机管理员的目的

-S
在一些情况下，nmap 可能无法确定你的源地址(nmap 会告诉你)。在这种情况使用这个选项给出你的 IP 地址。
在欺骗扫描时，也使用这个选项。使用这个选项可以让目标认为是其它的主机对自己进行扫描。

-e
告诉 nmap 使用哪个接口发送和接受数据包。nmap 能够自动对此接口进行检测，如果无效就会告诉你。

-g port
设置扫描的源端口。一些天真的防火墙和包过滤器的规则集允许源端口为 DNS(53)或者 FTP-DATA(20)的包通过和实现连接。显然，如果攻击者把源端口修改为 20 或者 53，就可以摧毁防火墙的防护。在使用 UDP 扫描时，先使用 53 号端口；使用 TCP 扫描时，先使用 20 号端口。注意只有在能够使用这个端口进行扫描时，nmap 才会使用这个端口。例如，如果你无法进行 TCP 扫描，nmap 会自动改变源端口，即使你使用了-g 选项。
对于一些扫描，使用这个选项会造成性能上的微小损失，因为我有时会保存关于特定源端口的一些有用的信息。

-r
告诉 nmap 不要打乱被扫描端口的顺序。

- randomize_hosts
使 nmap 在扫描之前，打乱每组扫描中的主机顺序，nmap 每组可以扫描最多 2048 台主机。这样，可以使扫描更不容易被网络监视器发现，尤其和 - scan_delay 选项组合使用，更能有效避免被发现。

-M
设置进行 TCP connect()扫描时，最多使用多少个套接字进行并行的扫描。使用这个选项可以降低扫描速度，避免远程目标宕机。

适时选项
通常，nmap 在运行时，能够很好地根据网络特点进行调整。扫描时，nmap 会尽量减少被目标检测到的机会，同时尽可能加快扫描速度。然而，nmap 默认的适时策略有时候不太适合你的目标。使用下面这些选项，可以控制 nmap 的扫描 timing：

-T
设置 nmap 的适时策略。Paranoid:为了避开 IDS 的检测使扫描速度极慢，nmap 串行所有的扫描，每隔至少 5 分钟发送一个包； Sneaky：也差不多，只是数据包的发送间隔是 15 秒；Polite：不增加太大的网络负载，避免宕掉目标主机，串行每个探测，并且使每个探测有 0.4 秒种的间隔；Normal:nmap 默认的选项，在不是网络过载或者主机/端口丢失的情况下尽可能快速地扫描；Aggressive:设置 5 分钟的超时限制，使对每台主机的扫描时间不超过 5 分钟，并且使对每次探测回应的等待时间不超过 1.5 秒钟；b>Insane:只适合快速的网络或者你不在意丢失某些信息，每台主机的超时限制是 75 秒，对每次探测只等待 0.3 秒钟。你也可是使用数字来代替这些模式，例如：-T 0 等于-T Paranoid，-T 5 等于-T Insane。
这些适时模式不能下面的适时选项组合使用。

- host_timeout
设置扫描一台主机的时间，以毫秒为单位。默认的情况下，没有超时限制。

- max_rtt_timeout
设置对每次探测的等待时间，以毫秒为单位。如果超过这个时间限制就重传或者超时。默认值是大约 9000 毫秒。

- min_rtt_timeout
当目标主机的响应很快时，nmap 就缩短每次探测的超时时间。这样会提高扫描的速度，但是可能丢失某些响应时间比较长的包。使用这个选项，可以让 nmap 对每次探测至少等待你指定的时间，以毫秒为单位。

- initial_rtt_timeout
设置初始探测的超时值。一般这个选项只在使用-P0 选项扫描有防火墙保护的主机才有用。默认值是 6000 毫秒。

- max_parallelism
设置最大的并行扫描数量。 - max_parallelism 1 表示同时只扫描一个端口。这个选项对其它的并行扫描也有效，例如 ping sweep, RPC scan。

- scan_delay
设置在两次探测之间，nmap 必须等待的时间。这个选项主要用于降低网络的负载。

例子
本节将由浅入深地举例说明如何使用 nmap。

nmap -vtarget.example.com
扫描主机 target.example.com 的所有 TCP 端口。-v 打开冗余模式。

nmap -sS -Otarget.example.com/24
发起对 target.example.com 所在网络上的所有 255 个 IP 地址的秘密 SYN 扫描。同时还探测每台主机操作系统的指纹特征。需要 root 权限。

nmap -sX -p22,53,110,143,4564 128.210.*.1-127
对 B 类 IP 地址 128.210 中 255 个可能的 8 位子网的前半部分发起圣诞树扫描。确定这些系统是否打开了 sshd、DNS、pop3d、imapd 和 4564 端口。注意圣诞树扫描对 Micro$oft 的系统无效，因为其协议栈的 TCP 层有缺陷。

nmap -v --randomize_hosts-p 80 ..2.3-5
只扫描指定的 IP 范围，有时用于对这个 Internet 进行取样分析。nmap 将寻找 Internet 上所有后两个字节是.2.3、.2.4、.2.5 的 IP 地址上的 WEB 服务器。如果你想发现更多有意思的主机，你可以使用 127-222，因为在这个范围内有意思的主机密度更大。

host -l company.com | cut-d -f 4 | ./nmap -v -iL -
列出 company.com 网络的所有主机，让 nmap 进行扫描。注意：这项命令在 GNU/Linux 下使用。如果在其它平台，你可能要使用其它的命令/选项
————————————————————