链滴

nmap 扫描命令常用示例

作者：lanlandezei
原文链接：https://ld246.com/article/1609211767893
来源网站：链滴

概述

Nmap代表Network Mapper，它是一个免费的开源网络发现和侦察工具，用于发现主机和收集有关机的详细信息。nmap是用C，C ++和Python编写的，最初于1997年9月发布，已经成为网络安全和字取证专业人士不可或缺的工具，依靠它们可以揭示有关目标主机和发掘潜在漏洞的详细信息。Nma揭示了诸如网络上的活动主机，打开的端口，操作系统和服务检测以及执行隐形扫描等信息。

1.扫描单个主机

nmap <ip地址>

示例

nmap 155.99.199.199

```
Starting Nmap 6.40 ( http://nmap.org ) at 2020-12-29 10:16 CST
Nmap scan report for 155.99.199.199.static.quadranet.com (155.99.199.199)
Host is up (0.017s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
873/tcp  open  rsync
3306/tcp open  mysql
```

可以指定域名，而不是指定IP地址

nmap <域名>

2.扫描多台主机

可以在一行中指定多个IP地址或域，并用空格隔开

nmap <ip1> <ip2>

指定IP地址范围

nmap 192.168.2.1-100

3.扫描子网

nmap 192.168.2.*

nmap 192.168.2.0/24

要优化扫描并仅发现子网中的活动主机，请使用-sP选项

nmap -sP 192.168.2.*

4.通过 -v 选项获取更多信息

nmap -v <ip>

5.扫描中排除主机

nmap 192.168.2.0/24 --exclude 192.168.2.20

要从Nmap扫描中排除多个主机，请在文件中指定要排除的主机，然后将命令链接到该文件

nmap 192.168.2.* --excludefile exclude.txt

上面的命令排除了exclude.txt文件中包含的所有主机

6.执行快速扫描

-F 选项来使用nmap进行更快的扫描

nmap -F <ip>

7. 扫描网络中的活动主机

这更像是ping扫描。它检测子网中的活动主机。要扫描活动主机，请传递-sn 选项，后跟IP地址和子网

nmap -sn 192.168.2.0/24

8.扫描文件中包含的主机

如果您有一个分段的网络，尤其是具有VLAN的分段网络，则可能主机位于不同的子网中。扫描它们一种简单方法是在文本文件中定义它们的IP地址，然后使用-iL选项将该文件作为参数传递

nmap iL hosts.txt

主机文件的示例

```
cat hosts.txt
192.168.2.100
192.168.2.102
192.168.20.5-50
```

9.执行扫描以检测防火墙

防火墙检测在执行漏洞测试或道德黑客攻击时特别有用。它使系统管理员可以知道是否启用了目标主的防火墙。要了解防火墙的状态，请使用-sA

nmap -sA 192.168.2.1

这将启动ACK扫描，以检查数据包是否可以未经过滤通过。使用-n标志可防止目标主机上的DNS反向析。

10.执行OS检测

Nmap还可以提供有关目标系统的OS或操作系统以及版本检测的见解。对于OS检测，请如图所示传递O选项。我们将扫描Linux系统上托管的云VPS，看看nmap给我们带来了什么。

nmap -O 176.113.66.112

Nmap会尽最大努力来识别操作系统及其版本，但是，结果可能并不总是代表准确的结果

11.执行端口扫描

nmap工具上的基本任务之一是扫描主机系统上的端口。您可以切入程序并使用-p标志后跟端口号指要扫描的端口

nmap -p 80 <ip>

另外，您可以通过使用逗号分隔多个端口来扫描多个端口

nmap -p 80,443 192.168.2.1

还可以通过用连字符分隔端口来定义要扫描的端口范围。

nmap -p 80-443 192.168.2.1

12.扫描TCP / UDP端口

可以缩小到扫描TCP或UDP端口。要扫描TCP端口，请使用-sT选项

nmap -sT 176.113.68.112

对于特定的TCP端口（例如端口80）

nmap -p T:80 176.113.68.112

对于UDP端口，请使用-sU选项

nmap -sU 176.113.68.112

对于特定的UDP端口，例如端口69

nmap -p U:69 176.113.68.112

13.收集系统服务版本和端口信息

扫描可能的漏洞时，检测正在运行的服务及其版本以及它们正在侦听的端口至关重要。这使您知道攻者可以利用哪些服务来破坏您的系统。有关服务和端口版本的知识使您可以决定是将服务更新为最新本还是完全卸载它们。

要收集服务和端口信息，请使用-sV标志

nmap -sV 176.113.68.112

14.执行隐形扫描

nmap扫描通常会有“噪音”，并留下痕迹，这些痕迹可以由功能强大的IDS（入侵检测系统）进行记，并最终可以追溯到您。要保持匿名，可以使用-sS选项执行隐形扫描 。

nmap -sS 176.113.68.112

15.确定支持的IP协议

可以使用-sO标志检索有关目标系统支持的协议（ICMP，TCP，UDP等）的信息

nmap -sO 176.113.68.112

16.执行主动扫描

使用-A选项时，nmap会给出非常详细的扫描结果，包括打开的端口和正在运行的服务的版本，操作统检测，甚至执行目标主机的跟踪路由。

nmap -A 176.113.68.112

17.将nmap输出保存到文件

默认情况下，nmap在终端上打印出扫描结果。但是，如果您需要将结果保存在文本文件中以便在方时进行更多分析，则可以使用所示的重定向操作符

nmap 176.113.68.112> scanme.txt

此外，您可以传递-oN选项，然后传递输出文件和主机。

nmap -oN scanme.txt scanme.nmap.org

18.nmap打印出主机接口和路由

有时，您可能会发现需要找到主机系统的接口和路由以进行调试。可以通过传递–iflist选项轻松实现

nmap --iflist

19.获得有关nmap的帮助

要满足您对其他nmap选项的好奇心，请使用-h标志。这与获得nmap命令的帮助同义。

nmap -h

20.检查nmap版本

要检查您正在使用的nmap版本，请运行以下命令

nmap -v

参考：https://www.iplayio.cn/post/704501286