1. 概述

Nmap 是一款开源免费的网络发现（Network Discovery）和安全审计（Security Auditing）工具。Nmap 是一个网络连接端扫描软件，用来扫描网上电脑开放的网络连接端。确定哪些服务运行在哪些连接端，并且推断计算机运行哪个操作系统（这是亦称 fingerprinting）。它是网络管理员必用的软件之一，以及用以评估网络系统安全。

上帝之眼　端口扫描非常牛

2. 基本功能

1）探测目标主机是否在线
2）扫描主机端口，嗅探所提供的网络服务
3）推断主机所用的操作系统
漏洞扫描

3. 工具安装

1）windows 操作系统 Nmap 工具安装

在 Nmap 官网 www.nmap.org 直接下载安装 Nmap 工具最新版本，如 nmap-7.80-setup.exe，双击进行安装，安装过程中会自动弹出安装 npcap-0.9982.exe 窗口，点击确认安装，并按照提示一步一步安装完成。

2）linux 操作系统 Nmap 工具安装

我们的 kali 系统是自带的

在 Nmap 官网 www.nmap.org 直接下载安装 Nmap 工具最新版本，如 nmap-7.80-1.x86_64.rpm，将工具安装包下载到本地，然后使用如下命令安装即可（切换到安装包目录）

安装命令：rpm -ivh nmap-7.80-1.x86_64.rpm
卸载命令：rpm -e nmap-7.80-1.x86_64.rpm

4. 扫描原理

4.1. TCP SYN 扫描（-sS）

Nmap 默认扫描方式，通常被称为半开放扫描。发送 SYN 包到目标端口，若收到 SYN/ACK 回复，则端口被认为开放状态；若收到 RST 回复，则端口被认为关闭状态；若没有收到回复，则认为该端口被屏蔽。因为仅发送 SYN 包对目标主机的特定端口，但不建立完整的 TCP 连接，所以相对比较隐蔽，而且效率比较高，适用范围广。

4.2. TCP connect 扫描（-sT）

使用系统网络 API connect 向目标主机的端口发起连接，如果无法连接，说明该端口关闭。该方式扫描速度比较慢，而且由于建立完整的 TCP 连接会在目标主机上留下记录信息，不够隐蔽。

4.3. TCP ACK 扫描(-sA)

向目标主机的端口发送 ACK 包，如果收到 RST 包，说明该端口没有被防火墙屏蔽；没有收到 RST 包，说明被屏蔽。该方式只能用于确定防火墙是否屏蔽某个端口，可以辅助 TCP SYN 的方式来判断目标主机防火墙的状况

4.4. TCP FIN/Xmas/NULL 扫描(-sN/sF/sX)

这三种扫描方式被称为秘密扫描，因为相对比较隐蔽。FIN 扫描向目标主机的端口发送的 TCP FIN 包括 Xmas tree 包或 NULL 包，如果收到对方的 RST 回复包，那么说明该端口是关闭的；没有收到 RST 包说明该端口可能是开放的或者被屏蔽了。其中 Xmas tree 包是指 flags 中 FIN URG PUSH 被置为 1 的 TCP 包；NULL 包是指所有的 flags 都为 0 的 TCP 包。

4.5. UDP 扫描(-sU)

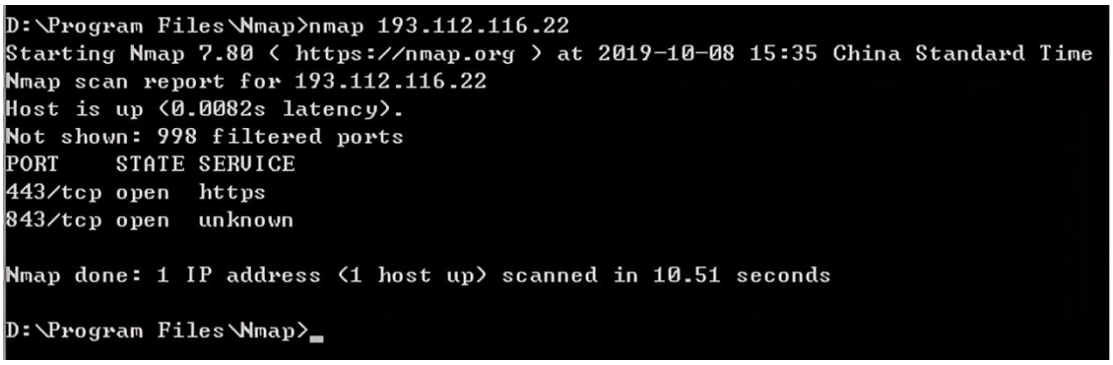
UDP 扫描用于判断 UDP 端口的情况，向目标主机的 UDP 端口发送探测包，如果收到回复 ICMP port unreachable 就说明该端口是关闭的；如果没有收到回复，那说明该 UDP 端口可能是开放的或者屏蔽的。因此，通过反向排除法的方式来判断哪些 UDP 端口是可能处于开放状态的。

4.6. 其他方式(-sY/-sZ)

除了以上几种常用的方式外，Nmap 还支持多种其他的探测方式。例如使用 SCTP INIT/Cookie-ECHO 方式是来探测 SCTP 的端口开放情况；使用 IP protocol 方式来探测目标主机支持的协议类型(tcp/udp/icmp/sctp 等等)；使用 idle scan 方式借助僵尸主机来扫描目标主机，以达到隐蔽自己的目的；或者使用 FTP bounce scan，借助 FTP 允许的代理服务扫描其他的主机，同样达到隐蔽自己的目的

5. 工具使用

1）直接使用 Nmap 命令行方式



2）使用 Zenmap 图形界面方式（详见 Zenmap 工具使用）

3）常见参数解读

0x01 目标规格

nmap 192.168.1.1	扫描一个 IP
nmap 192.168.1.1 192.168.2.1	扫描 IP 段
nmap 192.168.1.1-254	扫描一个范围
nmap nmap.org	扫描一个域名
nmap 192.168.1.0/24	使用 CIDR 表示法扫描
nmap -iL target.txt	扫描文件中的目标
nmap -iR 100	扫描 100 个随机主机
nmap --exclude 192.168.1.1	排除列出的主机

0x02 扫描手法

nmap 192.168.1.1 -sS	TCP SYN 端口扫描(有 root 权限默认)
nmap 192.168.1.1 -sT	TCP 连接端口扫描(没有 root 权限默认)
nmap 192.168.1.1 -sU	UDP 端口扫描
nmap 192.168.1.1 -sA	TCP ACK 端口扫描
nmap 192.168.1.1 -sW	滑动窗口扫描
nmap 192.168.1.1 -sM	TCP Maimon 扫描

0x03 扫描手法

nmap 192.168.1.1-3 -sL	不扫描,仅列出目标
nmap 192.168.1.1/24 -sn	只进行主机发现，禁用端口扫描
nmap 192.168.1.1-5 -Pn	跳过主机发现,直接扫描端口
nmap 192.168.1.1-5 -PS22-25,80	端口 X 上的 TCP SYN 发现,默认 80
nmap 192.168.1.1-5 -PA22-25,80	端口 X 上的 TCP ACK 发现,默认 80
nmap 192.168.1.1-5 -PU53	端口 X 上的 UDP 发现,默认 40125
nmap 192.168.1.1/24 -PR	本地网络上的 ARP 发现
nmap 192.168.1.1 -n	不做 DNS 解析

0x04 端口规格

nmap 192.168.1.1 -p 21	扫描特定端口
nmap 192.168.1.1 -p 21-100	扫描端口范围
nmap 192.168.1.1 -p U:53,T:21-25,80	扫描多个 TCP 和 UDP 端口

nmap 192.168.1.1 -p- 扫描所有端口
nmap 192.168.1.1 -p http,https 基于服务名称的端口扫描
nmap 192.168.1.1 -F 快速扫描(100 个端口)
nmap 192.168.1.1 --top-ports 2000 扫描前 2000 个端口
nmap 192.168.1.1 -p-65535 从端口 1 开始扫描

0x05 时间和性能

nmap 192.168.1.1 -T0 妄想症,非常非常慢，用于 IDS 逃逸
nmap 192.168.1.1 -T1 猥琐的,相当慢，用于 IDS 逃逸
nmap 192.168.1.1 -T2 礼貌的,降低速度以消耗更小的带宽，比默认慢十倍
nmap 192.168.1.1 -T3 正常的,默认，根据目标的反应自动调整时间模式
nmap 192.168.1.1 -T4 野蛮的,在一个很好的网络环境，请求可能会淹没目标
nmap 192.168.1.1 -T5 疯狂的,很可能会淹没目标端口或是漏掉一些开放端口

0x06 NSE 脚本

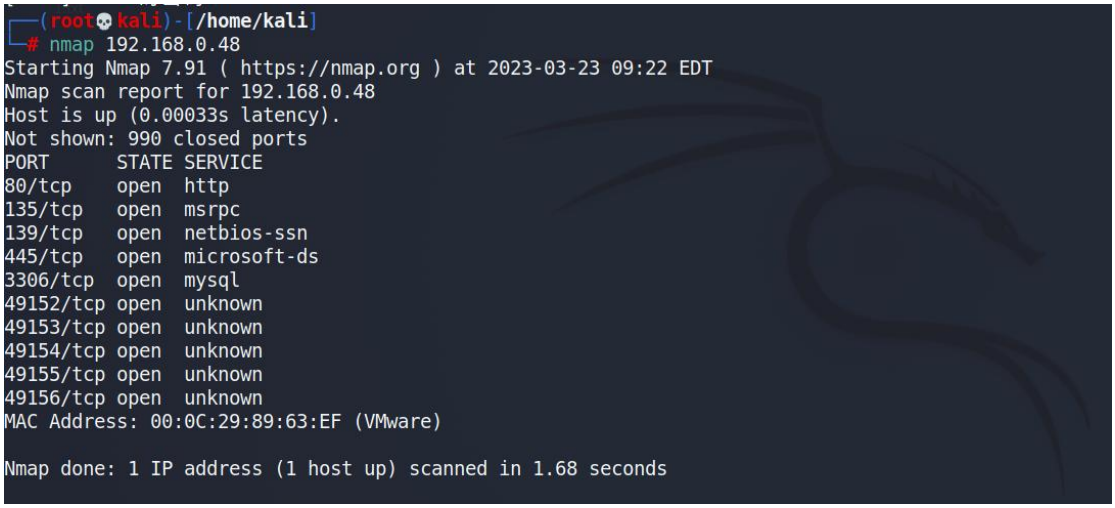
nmap 192.168.1.1 -sC 使用默认的 NSE 脚本进行扫描
nmap 192.168.1.1 --script=banner 使用单个脚本扫描,banner 示例
nmap 192.168.1.1 --script=http,banner 使用两个脚本扫描,示例 http,banner
nmap 192.168.1.1 --script=http* 使用通配符扫描,http 示例
nmap 192.168.1.1 --script "not intrusive" 扫描默认值,删除侵入性脚本
nmap 192.168.1.1 --script=smb-vuln* 扫描所有 smb 漏洞
nmap 192.168.1.1 --script=vuln 扫描常见漏洞

0x07 输出

nmap 192.168.1.1 -v 增加详细程度,-vv 效果更好
nmap 192.168.1.1 -oN test.txt 标准输出写入到指定文件中
nmap 192.168.1.1 -oX test.xml 将输入写成 xml 的形式
nmap 192.168.1.1 -oG grep.txt 将输出写成特殊格式
nmap 192.168.1.1 -oA results 将输出所有格式,有三种 .xml/.gnmap/.nmap
nmap 192.168.1.1 --open 仅显示开放的端口
nmap 192.168.1.1 -T4 --packet-trace 显示所有发送和接收的数据包
nmap --resume test.txt 恢复扫描，配合-oG 等命令使用

6. 扫描结果端口状态

1）open：端口是开放的
2）closed：端口是关闭的
3）filtered：端口被防火墙 IDS/IPS 屏蔽，无法确定其状态
4）unfiltered：端口没有被屏蔽，但是否开放需要进一步确定
5）open|filtered：端口是开放的或被屏蔽
6）closed|filtered ：端口是关闭的或被屏蔽


┌──(root💀kali)-[/home/kali]
└─# nmap 192.168.0.48
Starting Nmap 7.91 (https://nmap.org) at 2023-03-23 09:22 EDT
Nmap scan report for 192.168.0.48
Host is up (0.00033s latency).
Not shown: 990 closed ports
PORT   STATE SERVICE
80/tcp   open http
135/tcp   open msrpc
139/tcp   open netbios-ssn
445/tcp   open microsoft-ds
3306/tcp open mysql
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
MAC Address: 00:0C:29:89:63:EF (VMware)
Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds