nmap

BT5(BackTrack--Information Gathering--Network Analysis--Network Scanners-nmap)

-sP 渗透内网之后判断当前网络那些主机在线

nmap -sP 192.168.1/255

-vv 现实详细的扫描过程

-sS 使用 SYN 半开式扫描，这种扫描方式使得扫描结果更加正确(又称半开放,或

隐身扫描)

nmap -vv -sS IP

-O 大写 O 代表 OS 判断主机操作系统

nmap -O IP

延时策略

-T(0-5) 默认为 3

0 即 Paranoid 模式。为了避开 IDS 的检测使扫描速度极慢，nmap 串所有的扫描，

每隔至少 5 分钟发送一个包

1 即 Sneaky 模式。也差不多，只是数据包的发送间隔是 15 秒

2 即 Polite 模式。不增加太大的网络负载，串行每个探测，并使每个探测间隔

0.4 秒

3 即 Normal 模式。nmap 的默认选项，在不使网络过载或者主机/端口丢失的情况

下尽可能快速地扫描

4 即 Aggressive 模式。设置 5 分钟的超时限制，对每台主机的扫描时间不超过 5 分

钟，并且对每次探测回应的等待时间不超过 1.5 秒。

5 即 Insane 模式。只适合快速的网络或者不在意丢失默些信息，每台主机的超时

限制为 75 秒，对每次探测只等待 0.3 秒。

nmap -sS -T1 IP

-sV　　探测端口的服务类型/具体版本等信息

nmap -vv -sV IP

-p 端口号　对某个端口的服务版本进行详细探测 有助于升入的针对性攻击，

比如缓冲溢出攻击

nmap -vv -sV IP -p 21

适用于内外网的探测，以内网操作为示例(外网参数同)

简单端口扫描： nmap -vv -sT(sS、sF、sU、sA) 192.168.0.1 -D 127.0.0.1

(-D 伪造的地址)

OS 检测： nmap -vv -sS -O 192.168.0.1

RPC 鉴别： nmap -sS -sR 192.168.0.1 Linux 上的 portmap 就是一个简单的 RPC 服

务，监听端口为 111(默认)

Ping 扫射：nmap -sP 172.16.15.0/24

1)获取远程主机的系统类型及开放端口

Get info about remote host ports and OS detection

nmap -sS -P0 -sV -O <target>

这里的 < target > 可以是单一 IP，或主机名，或域名，或子网

-sS TCP SYN 扫描 (又称半开放,或隐身扫描)

-P0 允许你关闭 ICMP pings.

-sV 打开系统版本检测

-O 尝试识别远程操作系统

-sS TCP SYN scanning (also known as half-open, or stealth scanning)

-P0 option allows you to switch off ICMP pings.

-sV option enables version detection

-O flag attempt to identify the remote operating system

Other option:

-A 同时启用操作系统指纹识别和版本检测

-A option enables both OS fingerprinting and version detection

-v use -v twice for more verbosity.

nmap -sS -P0 -A -v < target >

2)列出开放了指定端口的主机列表

Get list of servers with a specific port open

nmap -sT -p 80 -oG – 192.168.1.* | grep open

Change the -p argument for the port number. See “man nmap” for

different ways to specify address ranges.

3)在网络寻找所有在线主机

Find all active IP addresses in a network

nmap -sP 192.168.0.*

或者也可用以下命令:

nmap -sP 192.168.0.0/24

指定 subnet

4)Ping 指定范围内的 IP 地址

Ping a range of IP addresses

nmap -sP 192.168.1.100-254

nmap accepts a wide variety of addressing notation, multiple

targets/ranges, etc.

5)在某段子网上查找未占用的 IP

Find unused IPs on a given subnet

nmap -T4 -sP 192.168.2.0/24 && egrep "00:00:00:00:00:00" /proc/net/arp

6)在局域网上扫找 Conficker 蠕虫病毒

Scan for the Conficker virus on your LAN ect.

nmap -PN -T4 -p139,445 -n -v –script=smb-check-vulns –script-args

safe=1 192.168.0.1-254

replace 192.168.0.1-256 with the IP's you want to check.

7)扫描网络上的恶意接入点 rogue APs.

Scan Network for Rogue APs.

nmap -A -p1-85,113,443,8080-8100 -T4 –min-hostgroup 50 –max-rtt-

timeout 2000 –initial-rtt-timeout 300 –max-retries 3 –host-timeout

20m –max-scan-delay 1000 -oA wapscan 10.0.0.0/8

I've used this scan to successfully find many rogue APs on a very,

very large network.

8)使用诱饵扫描方法来扫描主机端口

Use a decoy while scanning ports to avoid getting caught by the sys

admin

sudo nmap -sS 192.168.0.10 -D 192.168.0.2

Scan for open ports on the target device/computer (192.168.0.10) while

setting up a decoy address (192.168.0.2). This will show the decoy ip

address instead of your ip in targets security logs. Decoy address

needs to be alive. Check the targets security log at /var/log/secure

to make sure it worked.

9)为一个子网列出反向 DNS 记录

List of reverse DNS records for a subnet

nmap -R -sL 209.85.229.99/27 | awk '{if($3=="not")print"("$2") no

PTR";else print$3" is "$2}' | grep '('

10)显示网络上共有多少台 Linux 及 Win 设备?

How Many Linux And Windows Devices Are On Your Network?

sudo nmap -F -O 192.168.1.1-255 | grep "Running: " > /tmp/os; echo

"$(cat /tmp/os | grep Linux | wc -l) Linux device(s)"; echo "$(cat

/tmp/os | grep Windows | wc -l) Window(s) devices"