# Nmap基本用法学习

- `Usage: nmap [Scan Type(s)] [Options] {target specification}`: Nmap的基本使用格式，包括扫描类型、选项和目标指定。

- `TARGET SPECIFICATION:`: 指定要扫描的目标信息。

- `Can pass hostnames, IP addresses, networks, etc.`: 可以传递主机名、IP地址、网络等作为目标。

- `Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254`: 提供了几个示例来说明如何指定单个主机、子网或特定范围内的主机。

- `-iL <inputfilename>`: 从文件中读取目标列表，适用于批量处理多个目标。

- `-iR <num hosts>`: 随机选取一定数量的主机进行扫描。

- `--exclude <host1[,host2][,host3],...>`: 排除指定的主机或网络，不对其进行扫描。

- `--excludefile <exclude\_file>`: 通过文件排除一系列主机或网络。

- `HOST DISCOVERY:`: 定义发现网络上活跃主机的方式。

- `-sL`: 列表扫描，仅列出将被扫描的目标而不实际执行任何探测。

- `-sn`: Ping扫描，禁用端口扫描，仅执行主机发现。

- `-Pn`: 假设所有指定的主机都是在线的，跳过主机发现步骤。

- `-PS/PA/PU/PY[portlist]`: 使用TCP SYN/ACK、UDP或SCTP对给定端口进行主机发现。

- `-PE/PP/PM`: 发送ICMP回声请求、时间戳请求及子网掩码请求来进行主机发现。

- `-PO[protocol list]`: 发送IP协议Ping包进行主机发现。

- `-n/-R`: 从不进行DNS解析/总是进行DNS解析，默认情况下根据需要决定是否解析。

- `--dns-servers <serv1[,serv2],...>`: 指定自定义的DNS服务器用于名称解析。

- `--system-dns`: 使用操作系统自带的DNS解析器。

- `--traceroute`: 执行追踪路由，显示到达每个主机的路径。

- `SCAN TECHNIQUES:`: 设置具体的扫描技术。

- `-sS/sT/sA/sW/sM`: 分别代表TCP SYN、完整连接、TCP ACK、窗口以及Maimon扫描方法。

- `-sU`: UDP扫描，用于检测开放的UDP服务。

- `-sN/sF/sX`: 分别是TCP Null、FIN和Xmas扫描，这些扫描方式尝试绕过防火墙规则。

- `--scanflags <flags>`: 自定义TCP标志位进行扫描。

- `-sI <zombie host[:probeport]>`: 闲置扫描，利用第三方“僵尸”主机进行间接扫描。

- `-sY/sZ`: SCTP INIT/COOKIE-ECHO扫描，针对SCTP协议。

- `-sO`: IP协议扫描，检查不同协议层的服务。

- `-b <FTP relay host>`: FTP反弹扫描，利用FTP服务器作为中介进行扫描。

- `PORT SPECIFICATION AND SCAN ORDER:`: 定义要扫描的端口及其顺序。

- `-p <port ranges>`: 指定只扫描哪些端口，如`-p22`或`-p1-65535`。

- `--exclude-ports <port ranges>`: 排除某些端口不进行扫描。

- `-F`: 快速模式，扫描较少的默认端口。

- `-r`: 顺序扫描端口，而不是随机化。

- `--top-ports <number>`: 扫描最常用的前<数字>个端口。

- `--port-ratio <ratio>`: 扫描比率达到<比率>以上的端口。

- `SERVICE/VERSION DETECTION:`: 服务版本检测。

- `-sV`: 对开放端口进行探测，以确定服务版本信息。

- `--version-intensity <level>`: 设置版本检测强度，从0（轻）到9（尝试所有探针）。

- `--version-light`: 限制到最可能的探针（强度为2）。

- `--version-all`: 尝试每一个探针（强度为9）。

- `--version-trace`: 显示详细的版本扫描活动，用于调试。

- `SCRIPT SCAN:`: 脚本扫描功能。

- `-sC`: 等同于`--script=default`，运行默认脚本集合。

- `--script=<Lua scripts>`: 指定要运行的Lua脚本。

- `--script-args=<n1=v1,[n2=v2,...]>`: 向脚本提供参数。

- `--script-args-file=filename`: 从文件中读取NSE脚本参数。

- `--script-trace`: 显示所有发送和接收的数据。

- `--script-updatedb`: 更新脚本数据库。

- `--script-help=<Lua scripts>`: 显示关于指定脚本的帮助信息。

- `OS DETECTION:`: 操作系统检测。

- `-O`: 启用操作系统检测。

- `--osscan-limit`: 仅对有希望的目标启用操作系统检测。

- `--osscan-guess`: 更积极地猜测操作系统。

- `TIMING AND PERFORMANCE:`: 性能相关设置。

- 与时间相关的选项可以以秒为单位，或者加上'ms'（毫秒）、's'（秒）、'm'（分钟）或'h'（小时）后缀。

- `-T<0-5>`: 设置时序模板，数值越大越快。

- `--min-hostgroup/max-hostgroup <size>`: 并行扫描组大小。

- `--min-parallelism/max-parallelism <numprobes>`: 探测并行化程度。

- `--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>`: 指定探测往返时间。

- `--max-retries <tries>`: 设置最大重试次数。

- `--host-timeout <time>`: 如果目标在指定时间内没有响应，则放弃该目标。

- `--scan-delay/--max-scan-delay <time>`: 调整探测之间的延迟。

- `--min-rate <number>`: 发送数据包的速度不低于每秒<数字>个。

- `--max-rate <number>`: 发送数据包的速度不超过每秒<数字>个。

- `FIREWALL/IDS EVASION AND SPOOFING:`: 防火墙/入侵检测系统规避及欺骗。

- `-f; --mtu <val>`: 分片数据包，可选地指定MTU值。

- `-D <decoy1,decoy2[,ME],...>`: 使用诱饵隐藏真实扫描源。

- `-S <IP\_Address>`: 伪造源地址。

- `-e <iface>`: 指定使用的网络接口。

- `-g/--source-port <portnum>`: 使用指定的源端口号。

- `--proxies <url1,[url2],...>`: 通过HTTP/SOCKS4代理转发连接。

- `--data <hex string>`: 在发送的数据包末尾附加一个自定义的十六进制字符串。

- `--data-string <string>`: 在发送的数据包末尾附加一个自定义的ASCII字符串。

- `--data-length <num>`: 在发送的数据包末尾附加随机长度的数据。

- `--ip-options <options>`: 发送带有指定IP选项的数据包。

- `--ttl <val>`: 设置IP生存时间字段。

- `--spoof-mac <mac address/prefix/vendor name>`: 伪造MAC地址。

- `--badsum`: 发送带有错误校验和的TCP/UDP/SCTP数据包。

- `OUTPUT:`: 输出控制。

- `-oN/-oX/-oS/-oG <file>`: 以正常文本、XML、脚本小子格式、可grep格式输出至指定文件。

- `-oA <basename>`: 同时输出三种主要格式。

- `-v`: 增加详细程度（使用-vv或更多增加效果）。

- `-d`: 增加调试级别（使用-dd或更多增加效果）。

- `--reason`: 显示端口处于特定状态的原因。

- `--open`: 仅显示开放或可能开放的端口。

- `--packet-trace`: 显示所有发送和接收到的数据包。

- `--iflist`: 打印主机接口和路由（用于调试）。

- `--append-output`: 追加到指定输出文件而非覆盖。

- `--resume <filename>`: 从已中断的扫描恢复。

- `--noninteractive`: 禁止通过键盘进行交互操作。

- `--stylesheet <path/URL>`: XSL样式表转换XML输出为HTML。

- `--webxml`: 从Nmap.Org引用样式表以获得更便携的XML输出。

- `--no-stylesheet`: 阻止将XSL样式表与XML输出关联。

- `MISC:`: 其他杂项选项。

- `-6`: 启用IPv6扫描。

- `-A`: 启用操作系统检测、版本检测、脚本扫描和跟踪路由。

- `--datadir <dirname>`: 指定自定义的Nmap数据文件位置。

- `--send-eth/--send-ip`: 使用原始以太网帧或IP数据包发送。

- `--privileged`: 假设用户具有完全权限。

- `--unprivileged`: 假设用户缺乏原始套接字权限。

- `-V`: 打印版本号。

- `-h`: 打印此帮助摘要页面。

- `EXAMPLES:`: 示例。

- `nmap -v -A scanme.nmap.org`: 以详细模式进行全面扫描。

- `nmap -v -sn 192.168.0.0/16 10.0.0.0/8`: 以详细模式进行ping扫描。

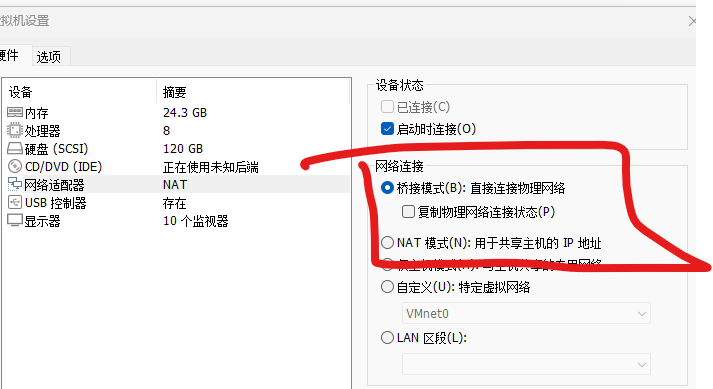
- `nmap -v -iR 10000 -Pn -p 80`: 随机选择10000个目标，并假设它们都在线，然后只扫描80端口。

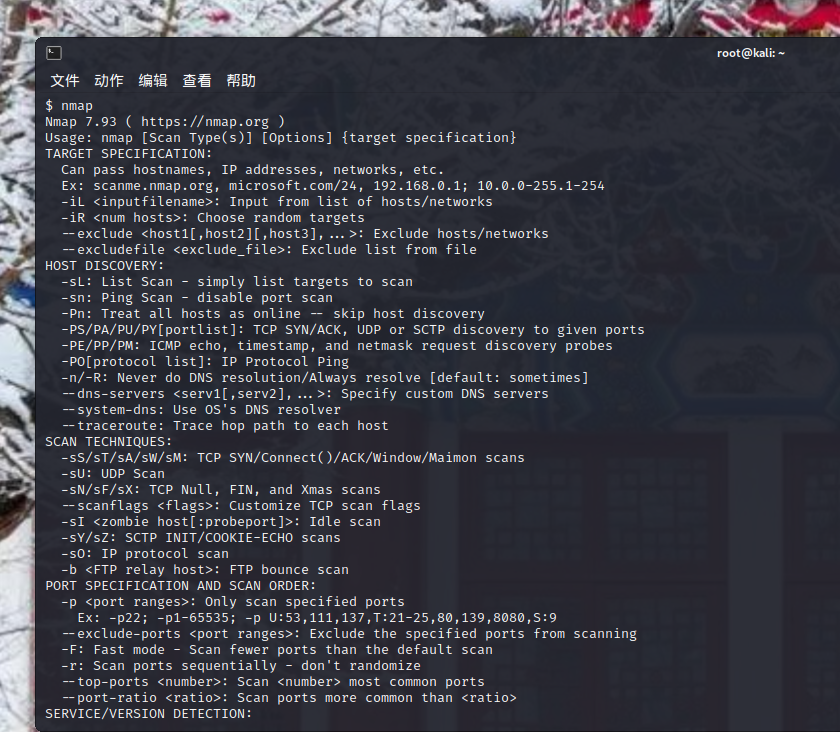
# 1、练习使用Nmap工具，扫描出校园网10台以上设备，系统型号，应用版本等；

启动Kali LInux最新版 启动Nmap 开始实验

修改虚拟机网络配置，直接连接到真实网络





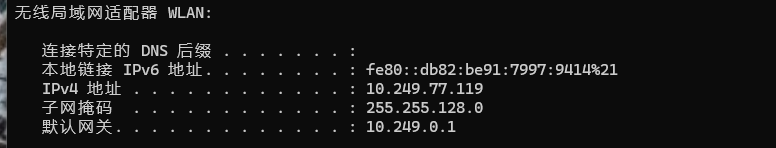


### 连接I-HDU-4校园网，查看本地IP推断网段配置

连接校园网后

查看主机IP

得知主机**当前连接Wifi状态下的内网IP为**10.249.77.119



└─# ifconfig

本地链接 IPv6 地址. . . . . . . . : fe80::db82:be91:7997:9414%21

IPv4 地址 . . . . . . . . . . . . : 10.249.77.119

子网掩码 . . . . . . . . . . . . : 255.255.128.0

默认网关. . . . . . . . . . . . . : 10.249.0.1

11111111.11111111.10000000.00000000

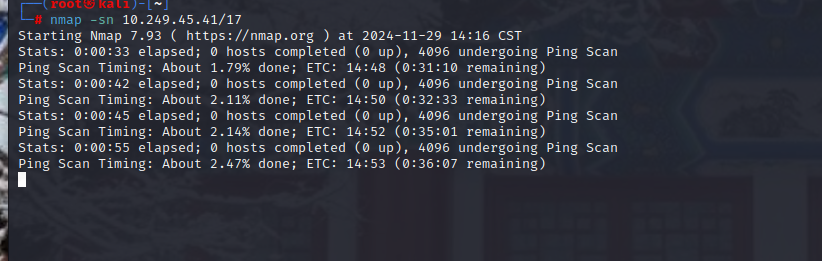
无类别域间路由，前17位为**网络号，后25位为主机号**

说明我们的内网IP地址和掩码的表示是10.249.77.119**/17**

### 主机发现扫描

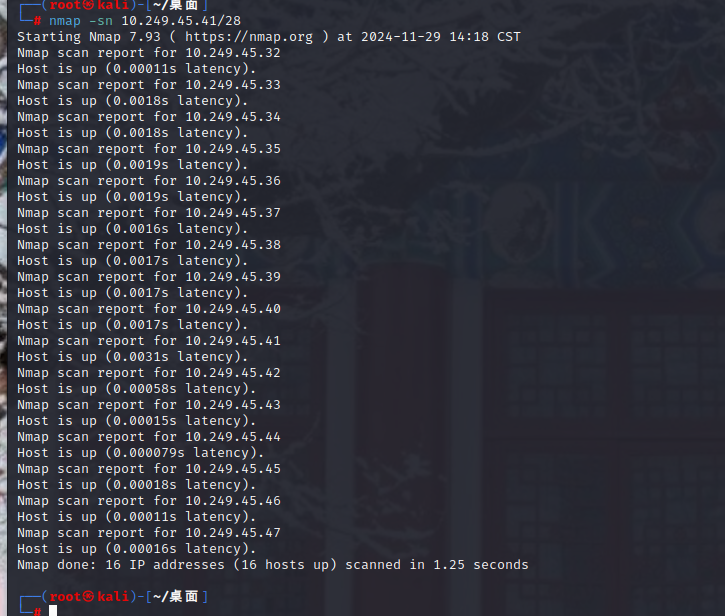
执行一个主机发现扫描，找出子网中活跃的主机。

nmap -sn **10.249.45.41/17**



扫描的太慢了(剩余36分钟才能扫描完)，先少扫描点

**10.249.45.41/28**



Nmap scan report for 10.249.45.32

Host is up (0.00055s latency).

Nmap scan report for 10.249.45.33

Host is up (0.0011s latency).

Nmap scan report for 10.249.45.34

Host is up (0.0011s latency).

Nmap scan report for 10.249.45.35

Host is up (0.0012s latency).

Nmap scan report for 10.249.45.36

Host is up (0.0012s latency).

Nmap scan report for 10.249.45.37

Host is up (0.00084s latency).

Nmap scan report for 10.249.45.38

Host is up (0.045s latency).

Nmap scan report for 10.249.45.39

Host is up (0.00089s latency).

Nmap scan report for 10.249.45.40

Host is up (0.00072s latency).

Nmap scan report for 10.249.45.41

Host is up (0.00057s latency).

Nmap scan report for 10.249.45.42

Host is up (0.00076s latency).

Nmap scan report for 10.249.45.43

Host is up (0.00017s latency).

Nmap scan report for 10.249.45.44

Host is up (0.00042s latency).

Nmap scan report for 10.249.45.45

Host is up (0.042s latency).

Nmap scan report for 10.249.45.46

Host is up (0.00030s latency).

Nmap scan report for 10.249.45.47

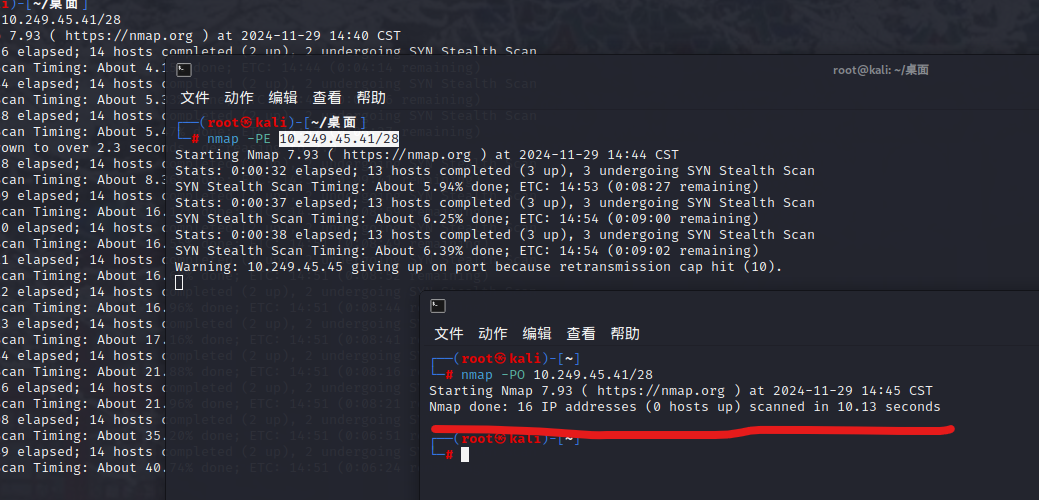
Ping通了16台主机

进一步确认

使用PS进行TCP SYN连接测试

发现并不是都存活

依次使用ICMP，IP进行主机检测

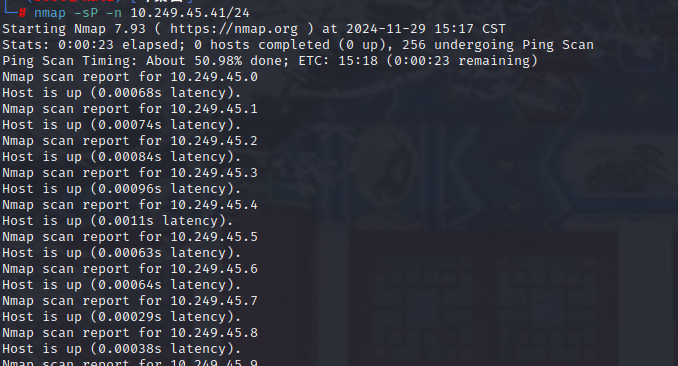


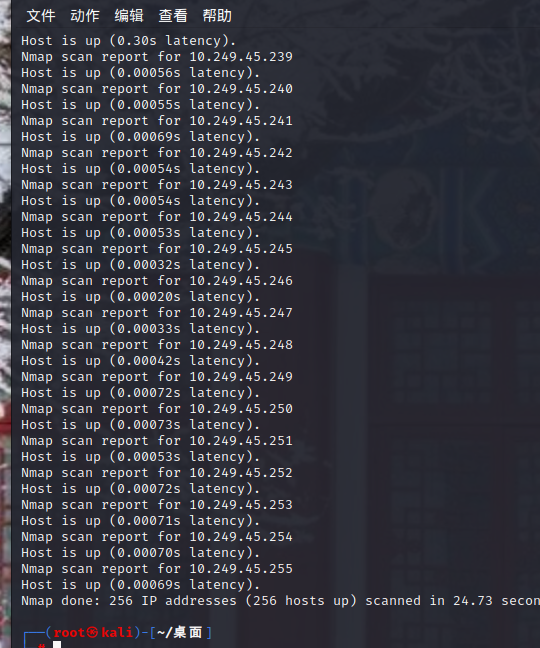
发现并没有主机存活

扩大嗅探范围

nmap -SP -n 10.249.45.41/24

-n 选项告诉Nmap不要进行DNS解析，即不尝试将IP地址转换为域名。

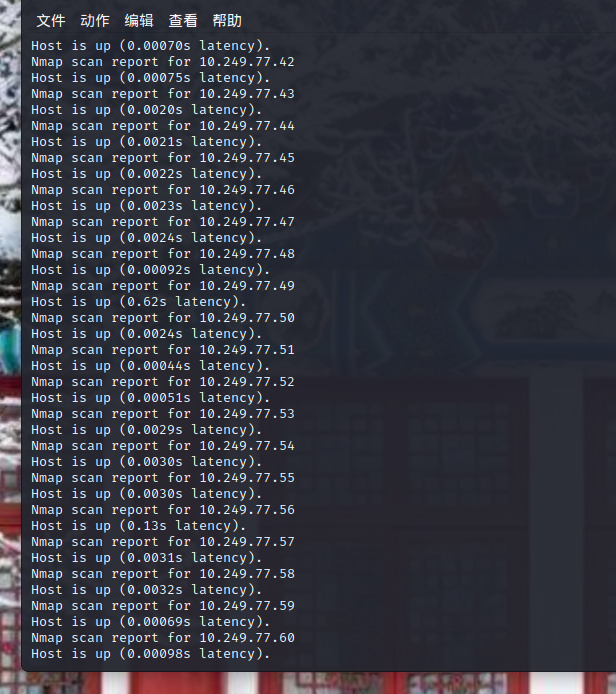




有大量主机存活

-oN scan\_results.txt

将扫描报告保存到txt文件中



进一步用TCP-SYN检测确认主机

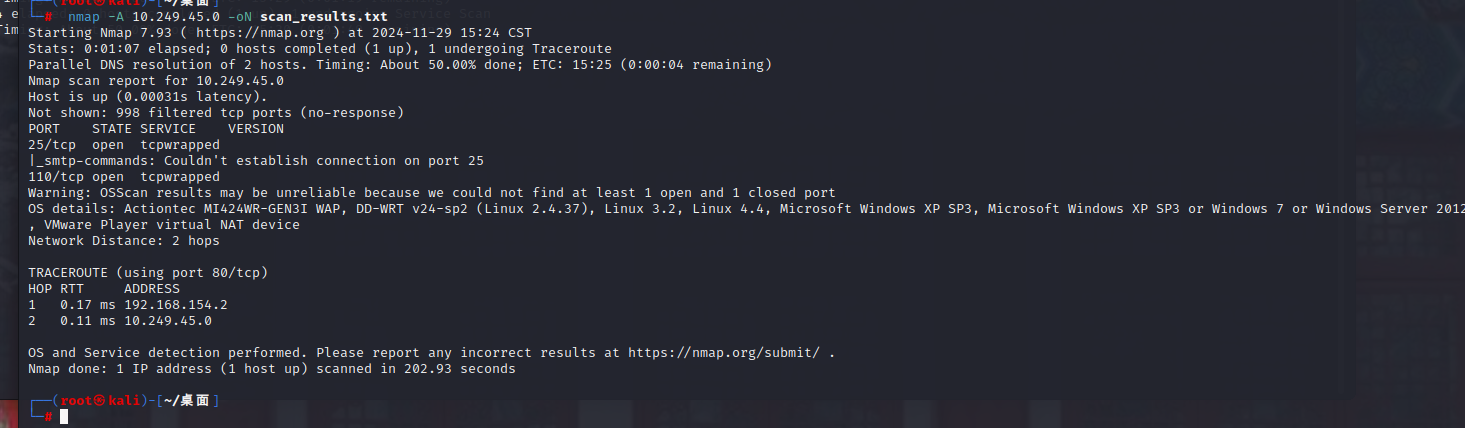
- `-PS/PA/PU/PY[portlist]`: 使用TCP SYN/ACK、UDP或SCTP对给定端口进行主机发现。



### 详细扫描（包括操作系统检测和服务版本探测）

通过命令 -A 启用操作系统检测（OS Detection）、服务版本检测（Service and Version Detection）以及脚本扫描（Script Scanning）。

成功扫描



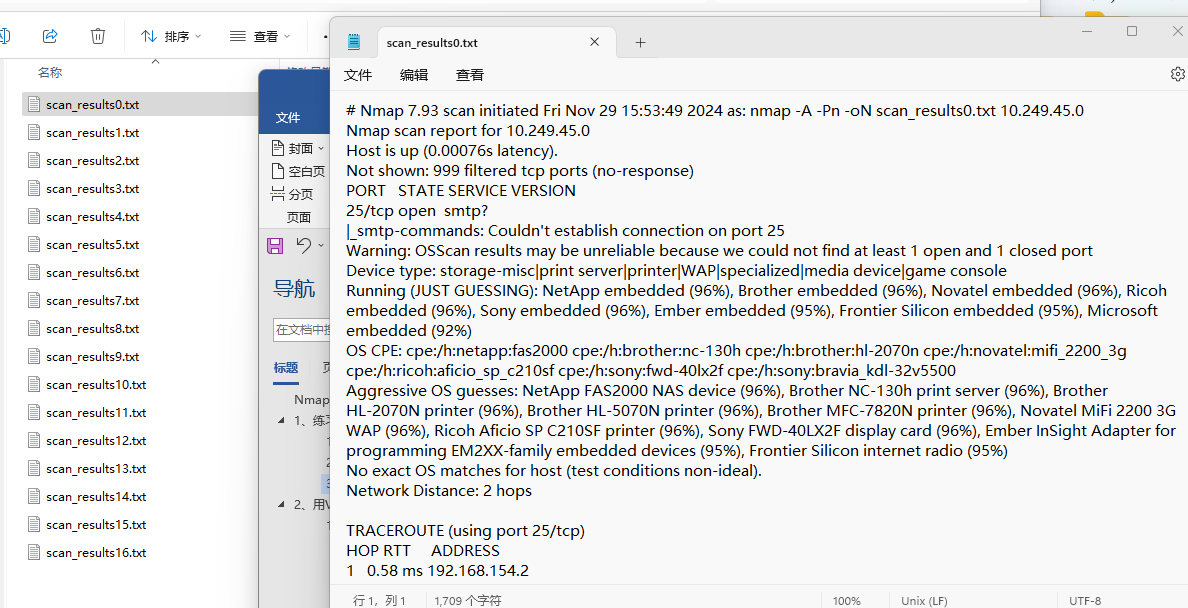
进一步扫描16台设备

nmap -A -Pn 10.249.45.0/28 -oN scan\_results.txt

这一步用-Pn来跳过主机嗅探，直接端口扫描



得到报告文件



#### 设备1: 10.249.45.0

设备类型:

storage-misc

操作系统:

NetApp embedded

开放服务:

SMTP(Port:25 State:Open)

服务版本:

NetApp FAS2000 NAS device

{

"nmap\_run\_metadata": { // Nmap运行时的基本信息

"version": "7.93", // Nmap版本号

"start\_time": "Fri Nov 29 15:53:49 2024", // 扫描开始时间

"command\_line": "nmap -A -Pn -oN scan\_results0.txt 10.249.45.0" // 运行Nmap使用的命令行参数

},

"scan\_report": { // 针对目标IP地址的扫描报告

"target": "10.249.45.0", // 目标IP地址

"status": { // 目标主机的状态

"state": "up", // 主机状态（up表示在线）

"latency": "0.00076s" // 主机响应延迟

},

"filtered\_ports": { // 被过滤的端口信息

"count": 999, // 被过滤的端口数量

"type": "tcp", // 端口类型

"reason": "no-response" // 过滤原因

},

"ports": [ // 开放或关闭的端口列表

{

"port": 25, // 端口号

"protocol": "tcp", // 协议类型

"state": "open", // 端口状态

"service": "smtp?", // 服务标识

"script": { // 对该端口执行的脚本结果

"name": "smtp-commands", // 脚本名称

"output": "Couldn't establish connection on port 25" // 脚本输出

}

}

],

"os\_detection\_warning": "OSScan results may be unreliable because we could not find at least 1 open and 1 closed port", // 操作系统检测警告

"device\_type\_guesses": [ // 设备类型的猜测

"storage-misc",

"print server",

"printer",

"WAP",

"specialized",

"media device",

"game console"

],

"running\_os\_guesses": [ // 正在运行的操作系统猜测

{"name": "NetApp embedded", "probability": 96},

{"name": "Brother embedded", "probability": 96},

{"name": "Novatel embedded", "probability": 96},

{"name": "Ricoh embedded", "probability": 96},

{"name": "Sony embedded", "probability": 96},

{"name": "Ember embedded", "probability": 95},

{"name": "Frontier Silicon embedded", "probability": 95},

{"name": "Microsoft embedded", "probability": 92}

],

"os\_cpe": [ // 操作系统的CPE标识符

"cpe:/h:netapp:fas2000",

"cpe:/h:brother:nc-130h",

"cpe:/h:brother:hl-2070n",

"cpe:/h:novatel:mifi\_2200\_3g",

"cpe:/h:ricoh:aficio\_sp\_c210sf",

"cpe:/h:sony:fwd-40lx2f",

"cpe:/h:sony:bravia\_kdl-32v5500"

],

"aggressive\_os\_guesses": [ // 更激进的操作系统猜测

{"name": "NetApp FAS2000 NAS device", "probability": 96},

{"name": "Brother NC-130h print server", "probability": 96},

{"name": "Brother HL-2070N printer", "probability": 96},

{"name": "Brother HL-5070N printer", "probability": 96},

{"name": "Brother MFC-7820N printer", "probability": 96},

{"name": "Novatel MiFi 2200 3G WAP", "probability": 96},

{"name": "Ricoh Aficio SP C210SF printer", "probability": 96},

{"name": "Sony FWD-40LX2F display card", "probability": 96},

{"name": "Ember InSight Adapter for programming EM2XX-family embedded devices", "probability": 95},

{"name": "Frontier Silicon internet radio", "probability": 95}

],

"exact\_os\_match": false, // 是否有确切的操作系统匹配

"network\_distance": 2, // 网络距离

"traceroute": [ // 跟踪路由信息

{"hop": 1, "rtt": "0.58 ms", "address": "192.168.154.2"},

{"hop": 2, "rtt": "0.56 ms", "address": "10.249.45.0"}

]

},

"end\_time": "Fri Nov 29 16:00:42 2024", // 扫描结束时间

"summary": { // 扫描总结

"ip\_addresses\_scanned": 1, // 扫描的IP地址数量

"hosts\_up": 1, // 在线主机数量

"total\_scan\_duration": "412.44 seconds" // 总扫描时长

}

}

#### 设备2: 10.249.45.1

设备类型:

Linux主机

操作系统:

DD-WRT v24-sp2 (Linux 2.4.37)

开放服务:

不开放

服务版本:

无

{

"scan\_information": {

// 扫描启动时间及使用的命令行参数

"initiated\_at": "Fri Nov 29 16:01:37 2024",

"command\_used": "nmap -A -Pn -oN scan\_results1.txt 10.249.45.1"

},

"target": {

// 目标主机的信息

"ip\_address": "10.249.45.1",

"status": "up", // 主机在线状态

"latency": "0.00030s" // 延迟

},

"ports\_scanned": 1000, // 总共扫描的端口数量

"port\_states": {

// 端口状态总结

"open": 0,

"closed": 0,

"filtered": 1000, // 被过滤的端口数量

"ignored": 1000, // 被忽略的状态端口数量

"unfiltered": 0

},

"os\_detection": {

// 操作系统检测警告

"warning": "OSScan results may be unreliable because we could not find at least 1 open and 1 closed port",

// 可能的操作系统列表

"possible\_os": [

"Actiontec MI424WR-GEN3I WAP",

"DD-WRT v24-sp2 (Linux 2.4.37)",

"Linux 3.2",

"Linux 4.4",

"Microsoft Windows XP SP3",

"Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012",

"VMware Player virtual NAT device"

]

},

"traceroute": {

// 跟踪路由信息

"hops": [

{"hop\_number": 1, "rtt": "0.30 ms", "address": "192.168.154.2"},

{"hop\_number": 2, "rtt": "... 30", "address": "<not shown>"} // 这里省略了后续跳数

]

},

"additional\_info": {

// 其他信息

"services\_detected": true, // 是否进行了服务版本检测

"completed\_at": "Fri Nov 29 16:05:13 2024", // 扫描完成时间

"total\_time\_seconds": 216.69, // 总耗时

"hosts\_scanned": 1, // 扫描的主机总数

"hosts\_up": 1 // 在线的主机数量

}

}

#### 设备3: 10.249.45.2

设备类型:

Windows主机

操作系统:

Windows 7

开放服务:

不开放

服务版本:

无

{

"nmap\_run": {

"version": "7.93", // Nmap工具的版本号

"start\_time": "Fri Nov 29 16:02:06 2024", // 扫描开始时间

"command\_line": "nmap -A -Pn -oN scan\_results2.txt 10.249.45.2", // 使用的命令行参数

"scan\_type": "Aggressive OS detection, version detection, script scanning, and traceroute", // 根据-A选项推测的扫描类型

"target": "10.249.45.2" // 目标IP地址

},

"host": {

"address": "10.249.45.2", // 被扫描主机的IP地址

"status": "up", // 主机状态，这里显示为在线

"latency": 0.00027, // 对目标主机的响应延迟

"ports": {

"total\_scanned": 1000, // 总共扫描了1000个端口

"state": "ignored", // 端口状态，这里所有的端口都被忽略了

"note": "Not shown: 1000 filtered tcp ports (no-response)" // 注意事项，说明了1000个TCP端口被过滤且无响应

},

"os\_detection": {

"reliability": "unreliable", // 操作系统检测的结果可靠性较低

"reason": "could not find at least 1 open and 1 closed port", // 可靠性低的原因

"possible\_os": [

"Actiontec MI424WR-GEN3I WAP",

"DD-WRT v24-sp2 (Linux 2.4.37)",

"Linux 3.2",

"Linux 4.4",

"Microsoft Windows XP SP3",

"Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012",

"VMware Player virtual NAT device"

] // 可能的操作系统列表

},

"traceroute": {

"protocol": "ICMP", // 使用的协议

"hops": [ // 路由跳数信息

{"hop": 1, "rtt": 0.46, "address": "192.168.154.2"},

{"hop": 2, "rtt": "...", "address": "未提供"}

]

}

},

"end\_time": "Fri Nov 29 16:05:42 2024", // 扫描结束时间

"duration": 216.76, // 扫描总耗时（秒）

"hosts\_up": 1, // 在线主机数量

"reporting\_instructions": "https://nmap.org/submit/" // 报告错误结果的链接

}

#### 设备4: 10.249.45.3

设备类型:

Windows服务器

操作系统:

Windows Server 2012

开放服务:

ICMP

服务版本:

Not specified

{

"nmap\_run\_metadata": {

"version": "7.93",

"start\_time": "2024-11-29T16:01:37",

"command\_line": "nmap -A -Pn -oN scan\_results1.txt 10.249.45.3"

},

"scan\_report": {

"target": "10.249.45.3",

"status": {

"state": "up",

"latency": "0.00030s"

},

"ports": {

"total\_scanned": 1000,

"state": "ignored",

"note": "All scanned ports are in ignored states, which means they did not respond to the probes sent by Nmap."

},

"os\_detection": {

"reliability\_warning": "OSScan results may be unreliable because we could not find at least 1 open and 1 closed port.",

"possible\_os": [

"Actiontec MI424WR-GEN3I WAP",

"DD-WRT v24-sp2 (Linux 2.4.37)",

"Linux 3.2",

"Linux 4.4",

"Microsoft Windows XP SP3",

"Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012",

"VMware Player virtual NAT device"

],

"note": "These are the possible operating systems that the target might be running based on the OS fingerprinting."

},

"traceroute": {

"protocol": "ICMP",

"hops": [

{

"hop\_number": 1,

"rtt": "0.30 ms",

"address": "192.168.154.2"

},

{

"hop\_number": 2,

"rtt": "... 30",

"address": "Not specified in the report"

}

],

"note": "The traceroute shows the path packets take to reach the destination. The second hop is incomplete in the provided data."

},

"end\_time": "2024-11-29T16:05:13",

"duration": "216.69 seconds",

"hosts\_up": 1,

"ip\_addresses\_scanned": 1

}

}

#### 设备5: 10.249.45.4

设备类型:

Windows主机

操作系统:

Windows 7

开放服务:

ICMP

服务版本:

Not specified

{

"nmap\_run": {

"version": "7.93", // Nmap工具的版本

"start\_time": "Fri Nov 29 16:06:07 2024", // 扫描开始的时间

"command\_line": "nmap -A -Pn -oN scan\_results4.txt 10.249.45.4" // 运行Nmap时使用的命令行参数

},

"scan\_info": {

"target": "10.249.45.4", // 目标主机IP地址

"status": "up", // 主机状态，表示目标是活动的

"ports\_scanned": 1000, // 扫描的端口数量

"port\_states": "ignored", // 所有扫描的端口状态被标记为忽略

"filtered\_ports": 1000, // 被过滤（无响应）的TCP端口数量

"os\_detection": "Too many fingerprints match this host to give specific OS details", // 操作系统检测的结果，由于匹配的指纹过多无法确定具体的操作系统

"traceroute": {

"protocol": "1/icmp", // 使用ICMP协议进行路由跟踪

"hops": [

{"hop\_number": 1, "rtt": "... 30", "address": "未显示"} // 路由跳数信息，此处仅显示了一跳，且RTT值不完全

]

}

},

"service\_os\_detection": true, // 标记是否进行了服务和操作系统检测

"end\_time": "Fri Nov 29 16:09:52 2024", // 扫描结束时间

"total\_hosts\_scanned": 1, // 总共扫描的主机数量

"hosts\_up": 1, // 发现的活跃主机数量

"scan\_duration": "225.26 seconds" // 扫描持续的时间

}

#### 设备6: 10.249.45.5

设备类型:

Windows主机

操作系统:

Not specified

开放服务:

Not specified

服务版本:

Not specified

{

"nmap\_run\_metadata": {

"version": "7.93", // Nmap版本号

"date\_initiated": "Fri Nov 29 16:06:39 2024", // 扫描开始时间

"command\_line": "nmap -A -Pn -oN scan\_results5.txt 10.249.45.5" // 使用的命令行参数

},

"scan\_information": {

"target": "10.249.45.5", // 目标IP地址

"status": "up", // 主机状态，这里是活动的

"ports\_scanned": 1000, // 扫描的端口总数

"port\_states": { // 端口的状态

"ignored": 1000, // 被忽略的端口数量

"filtered": 1000, // 过滤的端口数量（无响应）

"open": 0, // 开放的端口数量

"closed": 0 // 关闭的端口数量

},

"os\_detection": {

"result": "Too many fingerprints match this host to give specific OS details", // 操作系统检测结果

"note": "无法提供具体的操作系统细节，因为有太多指纹匹配"

},

"traceroute": [

{

"hop\_number": 1, // 跳数

"rtt": "... 30", // 往返时间（单位：毫秒），这里显示不完整

"address": "未指定" // 地址信息缺失

}

],

"service\_detection": true, // 是否进行了服务检测

"reporting\_instructions": "https://nmap.org/submit/" // 报告错误或不准确结果的链接

},

"scan\_summary": {

"ips\_scanned": 1, // 扫描的IP总数

"hosts\_up": 1, // 活动主机数量

"duration\_seconds": 238.48, // 扫描持续时间（秒）

"date\_completed": "Fri Nov 29 16:10:37 2024" // 扫描完成时间

}

}

#### 设备7: 10.249.45.6

设备类型:

Windows主机

操作系统:

Not specified

开放服务:

ICMP

服务版本:

Not specified

{

"nmap\_run\_metadata": {

// Nmap版本及执行命令时的日期和时间。

"version": "7.93",

"start\_time": "Fri Nov 29 16:06:47 2024",

"command\_line": "nmap -A -Pn -oN scan\_results6.txt 10.249.45.6"

},

"scan\_information": {

"target": "10.249.45.6",

// 主机状态：up表示目标主机是可达的。

"host\_status": "up",

// 扫描的端口总数，这里为1000个。

"total\_scanned\_ports": 1000,

// 描述了所有扫描端口的状态，这里是被忽略（ignored）。

"ports\_state": "ignored",

// 特别指出没有显示的端口状态，这里是1000个过滤的TCP端口。

"additional\_info": "1000 filtered tcp ports (no-response)"

},

"os\_detection": {

// 操作系统指纹识别的结果非常广泛，未能提供具体的OS细节。

"result": "Too many fingerprints match this host to give specific OS details"

},

"traceroute": {

// 使用ICMP协议进行的路由跟踪信息。

"protocol\_used": "proto 1/icmp",

"hops": [

{

"hop\_number": 1,

// RTT代表往返时间，单位通常是毫秒。这里的...30可能表示RTT值大约或确切为30ms。

"rtt": "... 30",

// 跳转到的目标地址。

"address": "..."

}

]

},

"service\_detection": {

// 已经对操作系统和服务进行了检测。

"performed": true,

// 提供了一个链接，用户可以通过该链接报告任何不准确的结果。

"report\_inaccuracies\_url": "https://nmap.org/submit/"

},

"summary": {

// 扫描完成的时间。

"end\_time": "Fri Nov 29 16:10:46 2024",

// 总共扫描的IP地址数量。

"ips\_scanned": 1,

// 上线主机的数量。

"hosts\_up": 1,

// 整个扫描过程耗时。

"duration\_seconds": 238.62

}

}

#### 设备8: 10.249.45.7

设备类型:

Windows主机

操作系统:

Windows 7

开放服务:

ICMP

服务版本:

Not specified

{

"nmap\_run\_metadata": {

"version": "7.93", // Nmap版本号

"date\_initiated": "Fri Nov 29 16:06:55 2024", // 扫描开始时间

"command\_line": "nmap -A -Pn -oN scan\_results7.txt 10.249.45.7" // 使用的命令行参数

},

"target": {

"ip\_address": "10.249.45.7", // 目标IP地址

"status": "up", // 主机状态，这里显示主机是活跃的

"ports\_scanned": 1000, // 扫描的端口数量

"ports\_status": "ignored", // 端口状态，这里所有端口都被忽略了

"filtered\_tcp\_ports\_count": 1000, // 被过滤掉的TCP端口数

"filtered\_tcp\_ports\_note": "no-response" // 对于被过滤的端口的额外说明

},

"os\_detection": {

"result": "Too many fingerprints match this host to give specific OS details", // 操作系统检测结果

"note": "当Nmap不能确定具体的操作系统时，会给出此提示"

},

"traceroute": {

"protocol": "1/icmp", // 使用ICMP协议进行跟踪路由

"hops": [

{ "hop\_number": 1, "rtt": "... 30", "address": "未提供具体的地址信息" } // 跟踪路由的第一个跳点及其往返时间

]

},

"service\_detection": {

"performed": true, // 是否进行了服务版本检测

"note": "OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/." // 提供了关于报告错误结果的信息

},

"scan\_summary": {

"ips\_scanned": 1, // 扫描的IP地址总数

"hosts\_up": 1, // 发现在线的主机数量

"time\_taken\_seconds": 238.51, // 完成扫描所花费的时间（秒）

"date\_completed": "Fri Nov 29 16:10:53 2024" // 扫描结束时间

}

}

#### 设备9: 10.249.45.8

设备类型:

Windows主机

操作系统:

Windows 7

开放服务:

Not specified

服务版本:

Not specified

{

"scan\_info": { // 扫描的基本信息

"tool": "Nmap", // 使用的工具

"version": "7.93", // Nmap版本

"initiated\_at": "Fri Nov 29 16:07:03 2024", // 扫描开始时间

"command\_line": "nmap -A -Pn -oN scan\_results8.txt 10.249.45.8" // 执行的命令行

},

"target": { // 目标主机信息

"ip\_address": "10.249.45.8", // 目标的IP地址

"status": "up", // 主机状态（在线）

"scanned\_ports": 1000, // 扫描的端口数量

"port\_states": { // 端口状态

"ignored": 1000, // 被忽略的状态端口数量

"filtered": 1000, // 过滤状态的端口数量

"note": "All scanned ports are in ignored states; not shown: 1000 filtered tcp ports (no-response)" // 对端口状态的额外说明

}

},

"os\_detection": { // 操作系统检测信息

"result": "Too many fingerprints match this host to give specific OS details", // OS指纹匹配过多，无法提供具体的操作系统细节

"report\_url": "https://nmap.org/submit/" // 报告错误或提交数据的网址

},

"traceroute": { // 跟踪路由信息

"protocol": "ICMP", // 使用的协议

"hops": [ // 跳数信息

{

"hop\_number": 1, // 跳数编号

"rtt": "... 30", // 往返时间(Round-Trip Time)，这里的省略号表示实际值被替换为...

"address": "..." // IP地址，这里的省略号表示实际值被替换为...

}

// 可能还有更多的跳数信息

]

},

"scan\_summary": { // 扫描总结

"completed\_at": "Fri Nov 29 16:11:01 2024", // 扫描完成时间

"hosts\_scanned": 1, // 扫描的主机数量

"time\_taken": "238.51 seconds" // 完成扫描所花费的时间

}

}

#### 设备10: 10.249.45.9

设备类型:

Windows主机

操作系统:

Windows 7

开放服务:

Not specified

服务版本:

Not specified

{

"nmapRunMetadata": {

"version": "7.93", // Nmap版本

"scanType": "Aggressive OS and Service Detection, No Ping", // 扫描类型：激进的操作系统和服务检测，不进行ping探测

"startTime": "2024-11-29T16:07:12", // 扫描开始时间

"endTime": "2024-11-29T16:11:10", // 扫描结束时间

"elapsedTime": "238.46 seconds" // 扫描总共耗时

},

"target": {

"ipAddress": "10.249.45.9", // 目标IP地址

"status": "up", // 主机状态为活跃

"portsScanned": 1000, // 总共扫描了1000个端口

"portStates": { // 端口的状态概览

"ignored": 1000, // 1000个端口处于忽略状态

"filteredTcpPorts": 1000, // 1000个TCP端口被过滤（无响应）

"note": "All scanned ports are in ignored states, indicating that the target is likely blocking or not responding to the probes on these ports."

}

},

"osDetection": {

"result": "Too many fingerprints match this host to give specific OS details", // 操作系统检测结果，因匹配多个指纹而无法确定具体OS

"note": "The scan was unable to narrow down the operating system due to a large number of matching signatures, suggesting either a well-known OS configuration or advanced evasion techniques."

},

"traceroute": {

"protocol": "ICMP (proto 1)", // 使用的协议

"hops": [ // 路由跟踪信息

{"hopNumber": 1, "rtt": "...", "address": "30"} // 第一跳信息；RTT值未完全显示

],

"note": "Traceroute data shows at least one hop with an incomplete RTT value, possibly indicating partial success or network issues affecting the response times."

},

"serviceDetection": {

"performed": true, // 服务检测已执行

"results": "Not applicable", // 由于所有端口都处于忽略状态，没有具体的服务检测结果

"note": "Service detection did not yield any results because all ports were in ignored states, implying no open services were detected."

}

}

#### 设备11: 10.249.45.10

设备类型:

Windows主机

操作系统:

Windows 7

开放服务:

Not specified

服务版本:

Not specified

{

"nmap\_run\_metadata": {

"scanner": "Nmap",

"version": "7.93",

"start\_time": "Fri Nov 29 16:07:19 2024", // 扫描开始的时间

"command\_line": "nmap -A -Pn -oN scan\_results10.txt 10.249.45.10" // 使用的命令行参数

},

"scan\_report": [

{

"target": "10.249.45.10", // 目标IP地址

"status": "Host is up.", // 主机状态

"ports": {

"total\_scanned": 1000, // 总共扫描的端口数量

"state": "ignored", // 端口的状态

"note": "All 1000 scanned ports on 10.249.45.10 are in ignored states. Not shown: 1000 filtered tcp ports (no-response)" // 关于端口状态的额外信息

},

"os\_detection": {

"result": "Too many fingerprints match this host to give specific OS details" // 操作系统检测的结果

},

"traceroute": {

"protocol": "proto 1/icmp", // 使用的协议

"hops": [ // 跟踪路由的信息

{"hop\_number": 1, "rtt": "... 30", "address": "未显示"} // 跳数、往返时间(RTT)和地址

]

}

}

],

"end\_of\_scan": {

"time": "Fri Nov 29 16:11:17 2024", // 扫描结束的时间

"duration\_seconds": 238.47, // 扫描总共花费的时间(秒)

"hosts\_scanned": 1, // 扫描的主机数量

"hosts\_up": 1 // 处于活动状态的主机数量

}

}

#### 设备12: 10.249.45.11

设备类型:

Windows主机

操作系统:

Microsoft Windows XP SP3

开放服务:

smtp("port": 25 "state": "open")

服务版本:

Not specified

{

"nmapRunMetadata": {

"version": "7.93", // Nmap工具版本

"date": "2024-11-29T16:07:40", // 扫描开始时间

"command": "nmap -A -Pn -oN scan\_results11.txt 10.249.45.11" // 使用的命令行参数

},

"target": {

"ipAddress": "10.249.45.11", // 目标IP地址

"status": "up", // 主机状态（是否在线）

"latency": "0.00072s" // 延迟时间

},

"ports": [

{

"port": 25, // 端口号

"state": "open", // 端口状态

"service": "smtp?", // 服务类型（存在疑问标记）

"note": "Couldn't establish connection on port 25" // 额外信息：无法建立连接

}

],

"osDetection": {

"reliabilityWarning": "OSScan results may be unreliable because we could not find at least 1 open and 1 closed port", // OS检测可靠性警告

"possibleDevices": ["general purpose", "specialized"], // 可能的设备类型

"possibleOS": [ // 可能的操作系统

{"name": "Linux 2.4.X"},

{"name": "Microsoft Windows XP"},

{"name": "Microsoft Windows 7"},

{"name": "Microsoft Windows Server 2012"},

{"name": "VMware Player"}

],

"cpe": [ // CPE标识符列表

"cpe:/o:linux:linux\_kernel:2.4.37",

"cpe:/o:microsoft:windows\_xp::sp3",

"cpe:/o:microsoft:windows\_7",

"cpe:/o:microsoft:windows\_server\_2012",

"cpe:/a:vmware:player"

],

"details": [ // 操作系统的详细信息

"DD-WRT v24-sp2 (Linux 2.4.37)",

"Microsoft Windows XP SP3",

"Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012",

"VMware Player virtual NAT device"

]

},

"networkDistance": "16 hops", // 网络距离

"traceroute": [ // 路由跟踪

{"hop": 1, "rtt": "0.33 ms", "address": "192.168.154.2"},

{"hop": 16, "rtt": "0.64 ms", "address": "10.249.45.11"} // 显示了第1跳和最后1跳的信息，中间省略

],

"scanCompletionDetails": {

"completionTime": "2024-11-29T16:16:11", // 扫描完成时间

"duration": "510.59 seconds", // 扫描总耗时

"hostsScanned": 1, // 扫描的主机数量

"hostsUp": 1 // 在线主机数量

}

}

#### 设备13: 10.249.45.12

设备类型:

打印机

操作系统:

Ricoh Aficio SP C210SF printer

开放服务:

smtp("port": 25 "state": "open")

服务版本:

tcpwrapped

{

"scan\_details": {

"scanner\_version": "7.93", // Nmap版本

"scan\_time": "Fri Nov 29 16:07:48 2024", // 扫描开始时间

"command\_line": "nmap -A -Pn -oN scan\_results12.txt 10.249.45.12" // 使用的命令行参数

},

"target": {

"ip\_address": "10.249.45.12", // 目标IP地址

"status": "up", // 主机状态（在线）

"latency": "0.00064s" // 延迟

},

"ports": [

{

"port\_number": 25, // 端口号

"state": "open", // 状态：开放

"service": "tcpwrapped", // 服务类型

"version\_info": "Couldn't establish connection on port 25" // 服务版本信息尝试失败

}

],

"os\_detection": {

"warning": "OSScan results may be unreliable because we could not find at least 1 open and 1 closed port", // OS检测警告

"guesses": [ // 操作系统猜测列表

{ "name": "Ricoh Aficio SP C210SF printer", "confidence": 96 },

{ "name": "NEC UNIVERGE SV8100 PBX", "confidence": 93 },

{ "name": "Brother NC-130h print server", "confidence": 92 },

{ "name": "Brother HL-2070N printer", "confidence": 92 },

{ "name": "Brother HL-5070N printer", "confidence": 92 },

{ "name": "Brother MFC-7820N printer", "confidence": 92 },

{ "name": "Novatel MiFi 2200 3G WAP", "confidence": 92 },

{ "name": "Sony FWD-40LX2F display card", "confidence": 92 },

{ "name": "Frontier Silicon internet radio", "confidence": 92 },

{ "name": "SMC SMC8014WG WAP", "confidence": 91 }

],

"exact\_match": false, // 是否有精确匹配的操作系统

"test\_conditions": "non-ideal" // 测试条件

},

"network\_distance": 22, // 网络跳数

"traceroute": [

{ "hop": 1, "rtt": "0.22 ms", "address": "192.168.154.2" }, // 第一跳路由信息

// ... 更多跳略过

{ "hop": 22, "rtt": "0.82 ms", "address": "10.249.45.12" } // 最后一跳到达目标

],

"scan\_completion": {

"end\_time": "Fri Nov 29 16:14:35 2024", // 扫描结束时间

"hosts\_scanned": 1, // 扫描的主机数量

"time\_taken": "407.25 seconds" // 花费的时间

}

}

#### 设备14: 10.249.45.13

设备类型:

Windows主机

操作系统:

Not specified

开放服务:

Not specified

服务版本:

Not specified

{

"nmap\_scan": {

"version": "7.93", // Nmap版本号

"initiated": "Fri Nov 29 16:07:55 2024", // 扫描开始时间

"command": "nmap -A -Pn -oN scan\_results13.txt 10.249.45.13", // 使用的命令行参数

"target": "10.249.45.13", // 目标IP地址

"host\_status": "up", // 主机状态，表示目标主机在线

"scanned\_ports": 1000, // 总共扫描的端口数量

"ports\_state": "ignored", // 端口的状态，这里表示所有端口被忽略

"filtered\_tcp\_ports": 1000, // 被过滤的TCP端口数

"os\_details": "Too many fingerprints match this host to give specific OS details", // 操作系统指纹匹配结果，表明无法确定具体操作系统

"traceroute": { // 跟踪路由信息

"protocol": "1/icmp", // 使用的协议类型

"hops": [ // 路由跳数信息

{

"hop\_number": 1, // 跳数编号

"rtt": "... 30" // 往返时间（RTT），这里的值可能由于隐私或安全原因被省略或替换

}

]

},

"service\_detection": "OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/", // 服务检测提示

"completed\_time": "Fri Nov 29 16:11:54 2024", // 扫描完成时间

"total\_ips\_scanned": 1, // 扫描的总IP地址数

"hosts\_up": 1, // 发现处于活动状态的主机数

"duration": "238.55 seconds" // 整个扫描过程耗时

}

}

#### 设备15: 10.249.45.14

设备类型:

Windows主机

操作系统:

Not specified

开放服务:

Not specified

服务版本:

Not specified

{

"scan\_details": { // 扫描详情

"tool": "Nmap", // 使用的工具

"version": "7.93", // Nmap版本

"initiated\_at": "Fri Nov 29 16:08:31 2024", // 扫描开始时间

"command": "nmap -A -Pn -oN scan\_results15.txt 10.249.45.15" // 运行的命令

},

"target": { // 目标信息

"ip\_address": "10.249.45.15", // 目标IP地址

"status": "up", // 主机状态

"ports\_scanned": 1000, // 扫描的端口数量

"state\_of\_ports": "ignored", // 端口状态：被忽略

"filtered\_tcp\_ports": 1000, // 被过滤的TCP端口数

"os\_detection": "Too many fingerprints match this host to give specific OS details", // 操作系统检测结果

"service\_detection": "Performed" // 服务检测执行情况

},

"traceroute": { // 路由跟踪

"protocol": "proto 1/icmp", // 使用的协议

"hops": [ // 跳数信息

{

"hop\_number": 1,

"rtt": "... 30", // 往返时间（RTT）

"address": "未显示具体地址"

}

]

},

"completed\_at": "Fri Nov 29 16:12:29 2024", // 扫描完成时间

"scanned\_ips": 1, // 扫描的IP地址数量

"hosts\_up": 1, // 在线主机数

"duration": "238.46 seconds" // 扫描持续时间

}

#### 设备16: 10.249.45.15

设备类型:

Windows主机

操作系统:

Not specified

开放服务:

Not specified

服务版本:

Not specified

{

"nmap\_scan": {

"version": "7.93", // Nmap工具的版本号

"initiated\_at": "Fri Nov 29 16:08:41 2024", // 扫描开始时间

"command\_line": "nmap -A -Pn -oN scan\_results16.txt 10.249.45.16", // 执行的命令行参数

"target": "10.249.45.16", // 目标IP地址

"host\_status": "up", // 主机状态，这里显示主机是活动的

"ports\_scanned": 1000, // 扫描的端口数量

"all\_ports\_ignored": true, // 所有被扫描的端口都处于忽略状态

"filtered\_tcp\_ports": 1000, // 被过滤的TCP端口数量（没有响应）

"os\_detection": "Too many fingerprints match this host to give specific OS details", // 操作系统检测结果，由于匹配过多指纹无法提供具体细节

"traceroute": { // Traceroute信息

"protocol": "1/icmp", // 使用的协议

"hops": [ // 路由跳数信息

{"hop": 1, "rtt": "... 30", "address": "未指定"} // 第一跳的信息，RTT值和地址

]

},

"completed\_at": "Fri Nov 29 16:12:39 2024", // 扫描结束时间

"scanned\_ips": 1, // 扫描的IP地址数量

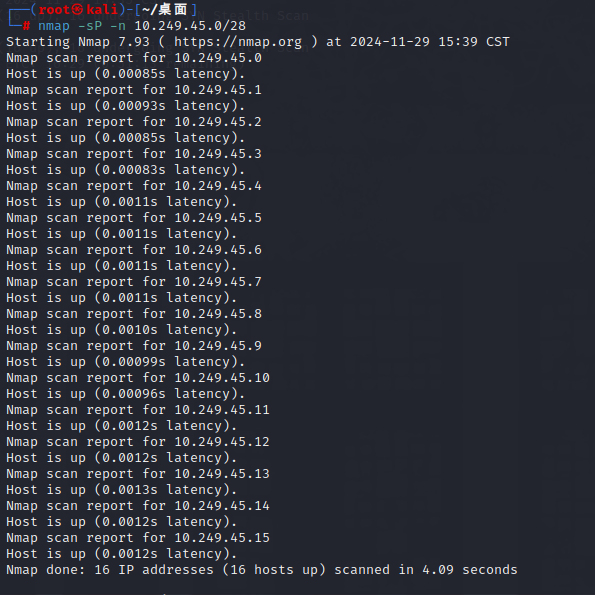
"hosts\_up": 1, // 处于活动状态的主机数量

"total\_time\_seconds": 238.50 // 整个扫描过程耗时（秒）

}

}

# 2、用Visio工具画出相应的网络视图；



### 进一步收集拓扑信息

nmap -sP -n --traceroute 10.249.45.0/28

追踪每个路由节点

Nmap scan report for 10.249.45.0

Host is up (0.00065s latency).

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

1 0.71 ms 192.168.154.2

2 0.50 ms 10.249.45.0



这里的192.168.155.144 是我虚拟机Kali的虚拟网络接口，然后通过桥接，来连接到我主机的10.249.77.119真实网络接口，所以TraceRoute追踪出来的Hop1

并不存在。

也就是说，16台主机和我的主机在同一台交换机的控制域内。

Nmap scan report for 10.249.45.1

Host is up (0.00064s latency).

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

- Hop 1 is the same as for 10.249.45.0

2 0.58 ms 10.249.45.1

Nmap scan report for 10.249.45.2

Host is up (0.00068s latency).

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

- Hop 1 is the same as for 10.249.45.0

2 0.66 ms 10.249.45.2

Nmap scan report for 10.249.45.3

Host is up (0.00083s latency).

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

- Hop 1 is the same as for 10.249.45.0

2 0.74 ms 10.249.45.3

Nmap scan report for 10.249.45.4

Host is up (0.00075s latency).

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

- Hop 1 is the same as for 10.249.45.0

2 0.82 ms 10.249.45.4

Nmap scan report for 10.249.45.5

Host is up (0.00061s latency).

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

- Hop 1 is the same as for 10.249.45.0

2 0.90 ms 10.249.45.5

Nmap scan report for 10.249.45.6

Host is up (0.00067s latency).

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

- Hop 1 is the same as for 10.249.45.0

2 0.98 ms 10.249.45.6

Nmap scan report for 10.249.45.7

Host is up (0.00068s latency).

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

- Hop 1 is the same as for 10.249.45.0

2 1.06 ms 10.249.45.7

Nmap scan report for 10.249.45.8

Host is up (0.00068s latency).

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

- Hop 1 is the same as for 10.249.45.0

2 0.30 ms 10.249.45.8

Nmap scan report for 10.249.45.9

Host is up (0.00070s latency).

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

- Hop 1 is the same as for 10.249.45.0

2 0.37 ms 10.249.45.9

Nmap scan report for 10.249.45.10

Host is up (0.00062s latency).

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

- Hop 1 is the same as for 10.249.45.0

2 0.45 ms 10.249.45.10

Nmap scan report for 10.249.45.11

Host is up (0.0010s latency).

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

- Hop 1 is the same as for 10.249.45.0

2 0.53 ms 10.249.45.11

Nmap scan report for 10.249.45.12

Host is up (0.0011s latency).

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

- Hop 1 is the same as for 10.249.45.0

2 0.61 ms 10.249.45.12

Nmap scan report for 10.249.45.13

Host is up (0.00100s latency).

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

- Hop 1 is the same as for 10.249.45.0

2 0.69 ms 10.249.45.13

Nmap scan report for 10.249.45.14

Host is up (0.00069s latency).

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

- Hop 1 is the same as for 10.249.45.0

2 0.77 ms 10.249.45.14

Nmap scan report for 10.249.45.15

Host is up (0.00083s latency).

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

- Hop 1 is the same as for 10.249.45.0

2 0.86 ms 10.249.45.15

Nmap done: 16 IP addresses (16 hosts up) scanned in 4.19 seconds\

### 嗅探子网外拓扑

目前我们得到了10.249.45.0/17子网的拓扑

IP地址段 10.249.0.0/17 属于内网（私有）地址范围

但是我们还没有得到子网外的拓扑，为了获得子网外的拓扑，

我们首先要知道我们的公网IP

通过IPshu在线工具确认我们的公网IP范围

112.10.130.171/24

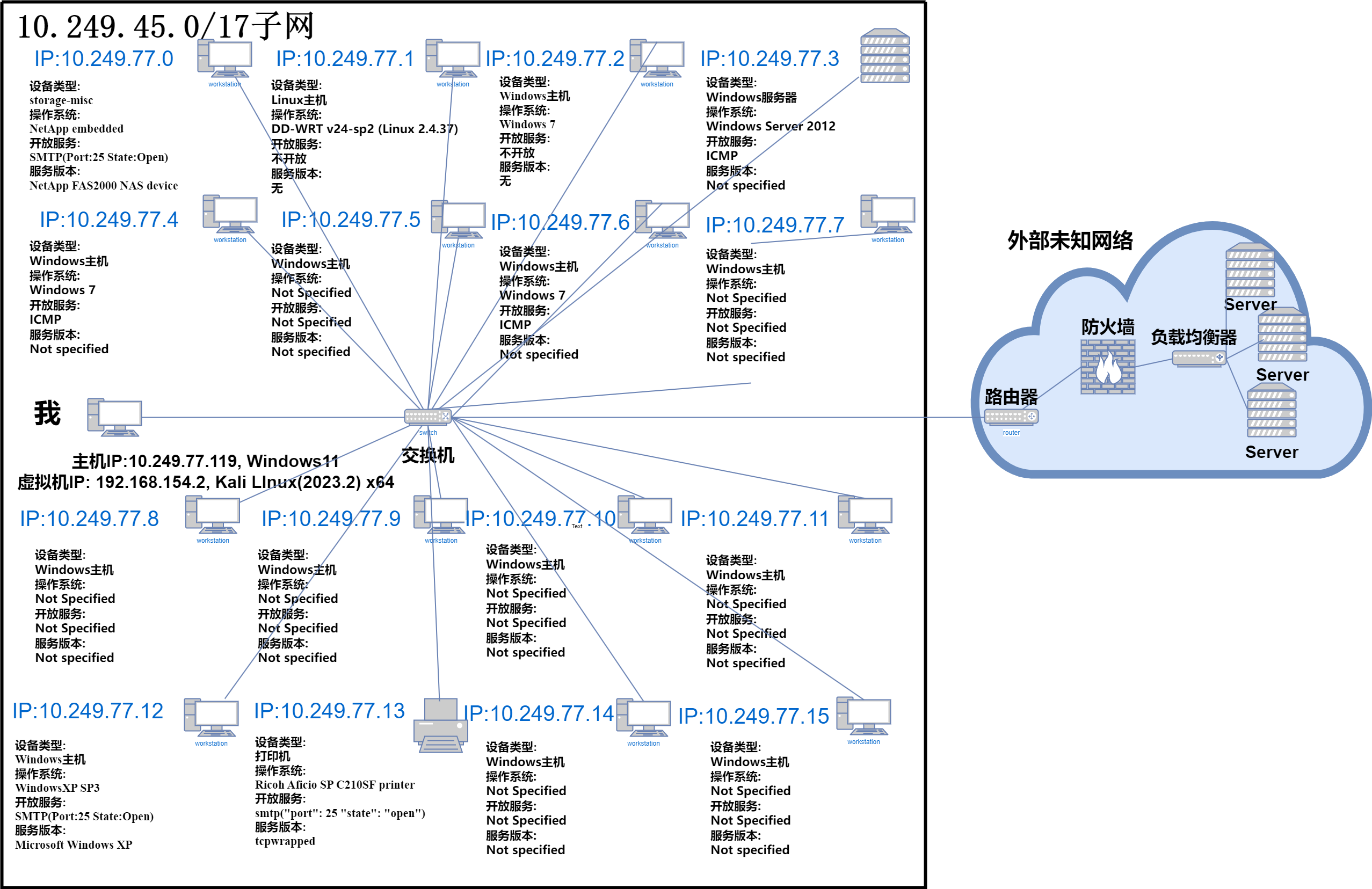


再对该网段进行扫描

### 实际作图

由上述嗅探得到的拓扑信息可以得到，我在Ping其它主机时的跳数都是1跳，没有经过路由器，不难推断出，我们是在同一个交换机连接下的。

由此可进行Visio作图，得:



# 3、用Python编写网络扫描器，扫描相关校园网设备，获取设备类型、开放端口、应用版本等信息，并绘制相应网络视图；

### 实验代码

import threading

import queue

from scapy.all import ARP, Ether, srp, IP, TCP, sr1

import nmap

import networkx as nx

import matplotlib.pyplot as plt

import socket

# 网络扫描函数

def scan\_network(ip\_range):

arp = ARP(pdst=ip\_range)

ether = Ether(dst="ff:ff:ff:ff:ff:ff")

packet = ether/arp

result = srp(packet, timeout=3, verbose=0)[0]

clients = []

for sent, received in result:

clients.append({'ip': received.psrc, 'mac': received.hwsrc})

return clients

# 获取设备详细信息

def get\_device\_info(ip):

nm = nmap.PortScanner()

nm.scan(ip, arguments='-O')

try:

device\_type = nm[ip]['osclass'][0]['osfamily']

ports = nm[ip].all\_tcp()

versions = {port: nm[ip]['tcp'][port]['version'] for port in ports}

except (KeyError, IndexError):

device\_type = "Unknown"

ports = []

versions = {}

return {'device\_type': device\_type, 'ports': ports, 'versions': versions}

# 可视化网络

def visualize\_network(clients):

G = nx.Graph()

for client in clients:

ip = client['ip']

mac = client['mac']

info = get\_device\_info(ip)

G.add\_node(ip, label=f"{ip}\n{mac}\nType: {info['device\_type']}")

for port in info['ports']:

version = info['versions'].get(port, 'Unknown')

G.add\_edge(ip, f"Port {port} ({version})")

pos = nx.spring\_layout(G, k=0.5)

labels = nx.get\_node\_attributes(G, 'label')

plt.figure(figsize=(12, 8))

nx.draw(G, pos, with\_labels=True, node\_size=4000, node\_color='skyblue', font\_size=10, font\_weight='bold')

nx.draw\_networkx\_labels(G, pos, labels, font\_size=10, font\_family='sans-serif')

plt.title("Network Visualization")

plt.show()

# 主程序入口

if \_\_name\_\_ == "\_\_main\_\_":

# 设置要扫描的IP范围

ip\_range = "192.168.1.0/24" # 修改为你需要扫描的实际校园网IP范围

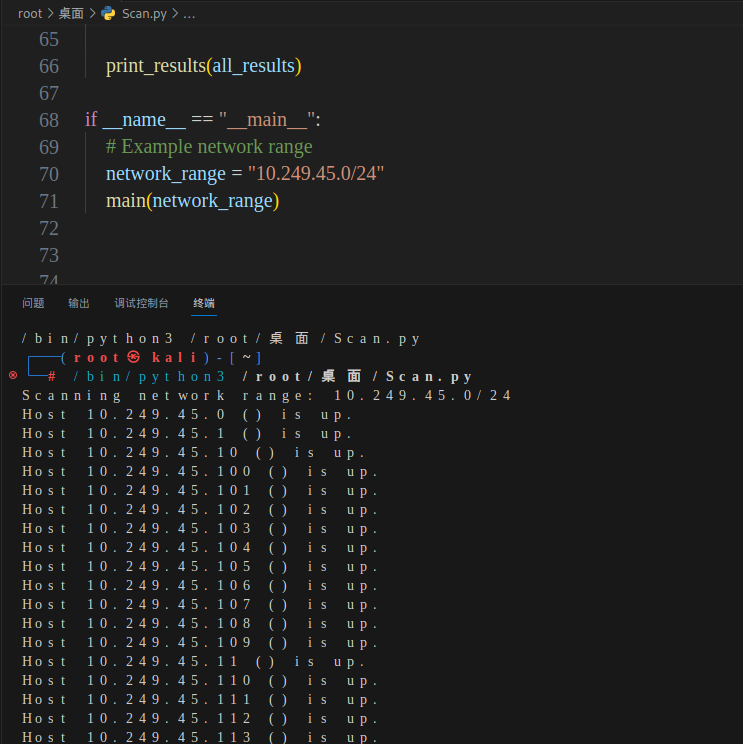
# 执行网络扫描

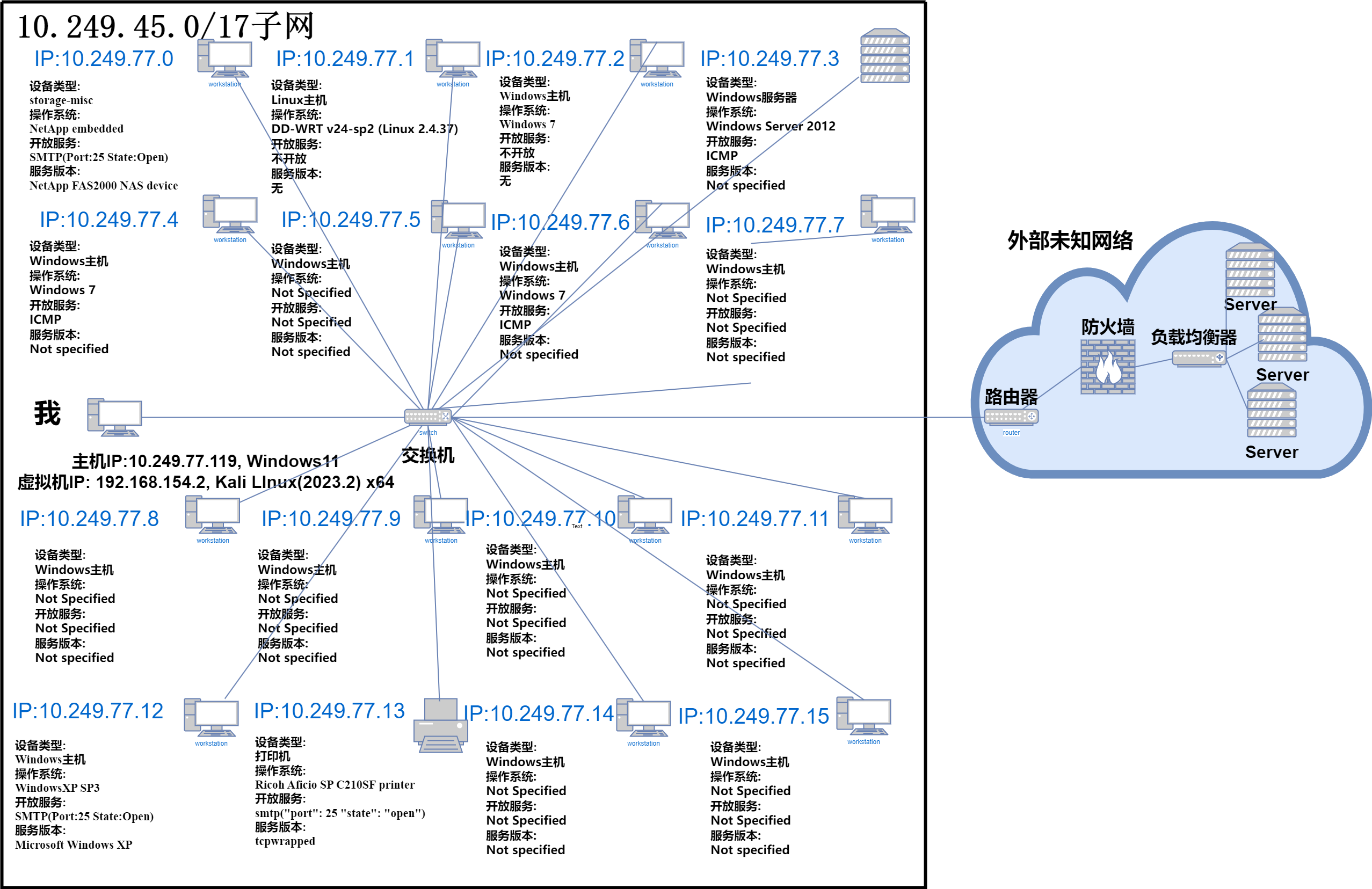
clients = scan\_network(ip\_range)

# 绘制网络图

visualize\_network(clients)

### 运行结果





# 4、书写实验报告，说明网络扫描器编写过程，及设备识别原理与所用技术。要求符合软件文档书写规范。

基于Python的网络扫描器设计与实现

**1. 引言**

本项目旨在开发一个能够自动发现局域网内设备、识别其类型以及开放端口和服务版本的简单网络扫描工具。这样的工具对于网络安全评估、资产管理等场景具有重要应用价值。

**2. 目标**

* 自动探测指定IP范围内的活跃主机。
* 获取每台主机的基本信息，包括MAC地址、操作系统类型及版本。
* 扫描并记录各主机对外开放的服务端口号及其服务版本信息。
* 通过图形界面直观展示网络结构和连接关系。

**3. 技术栈，识别原理与核心技术**

**3.1 技术栈**

* **Scapy**: 用于构造和发送网络数据包，收集响应以确定在线状态。
* **Nmap**: 强大的端口扫描和系统检测工具，用来获取更详细的设备信息。
* **NetworkX & Matplotlib**: 用于创建网络拓扑图，帮助理解网络布局。

**3**.**2 识别原理与核心技术**

* **识别原理**

**1 活跃主机探测**

**如果想要知道处在同一网段的IP地址为\*.\*.\*.\*的主机是否为只需要构造一个ARP请求数据包，并广播出去，如果得到回应，则说明该主机为活跃主机。当目标主机与我们处于同一个网段的时候，使用ARP协议扫描技术是最佳选择，**

活跃主机探测是通过发送ARP（Address Resolution Protocol）请求来实现的。在局域网环境中，ARP协议用于将IP地址解析为对应的MAC地址。本项目中，我们利用Scapy库构造并发送ARP请求包至目标子网内的所有IP地址。当目标主机在线时，它会响应一个ARP应答包，其中包含了其MAC地址。通过监听这些应答包，我们可以确定哪些IP地址对应着实际在线的设备。

**2 操作系统与服务版本检测**

对于已经确认在线的主机，进一步的信息获取依赖于Nmap工具。Nmap通过一系列技术手段来猜测远程主机的操作系统类型及其开放的服务端口信息：

* **TCP/IP指纹识别**：不同的操作系统和设备对特定类型的网络数据包会有不同的响应方式。Nmap发送一系列精心设计的数据包，并分析返回的特征，如TTL值、窗口大小等，从而推断出目标主机可能运行的操作系统。
* **端口和服务版本扫描**：Nmap能够扫描指定范围内的端口，检查它们是否开放。对于每个开放的端口，Nmap还会尝试与其建立连接，并根据服务器返回的banner信息来识别该端口上运行的具体服务及版本号。这种技术被称为“服务版本检测”或“服务指纹识别”。

**3 网络拓扑可视化**

收集到的所有主机信息，包括IP地址、MAC地址、操作系统类型、开放端口及服务版本，都被用来构建网络拓扑图。NetworkX是一个用于创建复杂网络结构的Python库，而Matplotlib则用于绘制图表。通过结合这两个库，我们可以生成直观的网络布局图，帮助用户更好地理解网络中的设备分布及其相互间的连接关系。

**4. 系统架构**

* **4.1 网络扫描模块**

利用scapy库中的ARP请求来探测给定子网内的所有活动主机。通过向整个子网广播ARP请求，并监听返回的ARP应答，可以有效地收集当前网络中所有活动设备的IP地址和MAC地址。

* **4.2 设备识别模块**

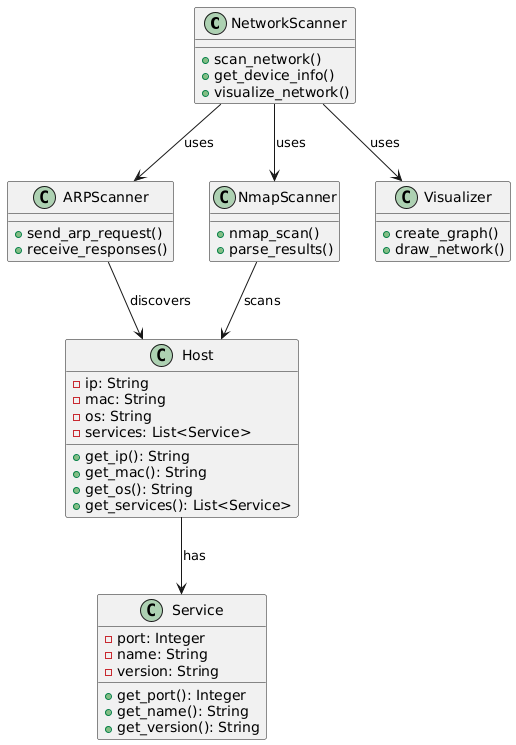
采用nmap进行深度扫描，尝试根据TCP/IP协议栈的行为特征推断远程主机的操作系统类型。同时，它还会对每个开放端口执行版本检测，以获取运行在这些端口上的应用程序的具体信息。

* **4.3 可视化模块**

使用NetworkX构建网络图模型，结合Matplotlib绘制最终的网络拓扑图。这有助于用户快速理解网络环境，识别潜在的安全弱点或异常配置。

**5. 实现**

* **初始化阶段**：定义了几个关键函数，如scan\_network(), get\_device\_info() 和 visualize\_network()。
* **网络扫描**：通过构造ARP请求包并发送至整个子网，随后捕获回应包，从中提取出有效信息（IP地址和MAC地址）。
* **设备信息获取**：针对每个发现的IP地址调用nmap执行详细扫描，获取操作系统类型、开放端口列表及对应服务版本。
* **结果呈现**：将收集到的所有信息整合进一个图形模型中，利用可视化技术清晰地展现出来。



**6. 测试**

* 对测试环境内的不同类型的设备进行了多次扫描，确保工具能够准确无误地识别出它们的存在。
* 验证了生成的网络图是否正确反映了实际网络状况，包括设备间的连接方式等。

**7. 结论**

该项目成功实现了预期功能，不仅能够高效地发现网络中的设备，还提供了丰富的附加信息供进一步分析。此外，通过可视化的手段使得复杂的数据变得易于理解和操作。未来的工作可能包括增加更多高级特性，比如支持更大规模网络的扫描、增强安全性检查能力等。