信息安全的艺术　实验四

PB23010356 张竞一
学院：数学科学学院

2025 年 11 月 6 日

1　实验目的

1. 熟悉并掌握 Angry IP Scanner 的基本使用方法
2. 熟悉并掌握 Nmap 命令行工具的基本使用方法
3. 了解网络扫描在信息安全中的应用

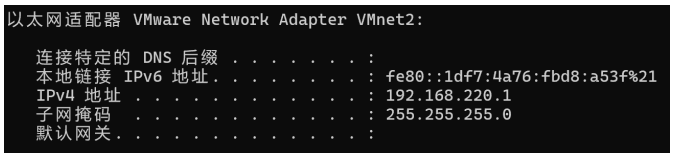
2　实验环境

- 操作系统：Windows 11
- 工具软件：
  - Angry IP Scanner v3.9.2
  - Nmap 7.98

3　Angry IP Scanner 扫描结果

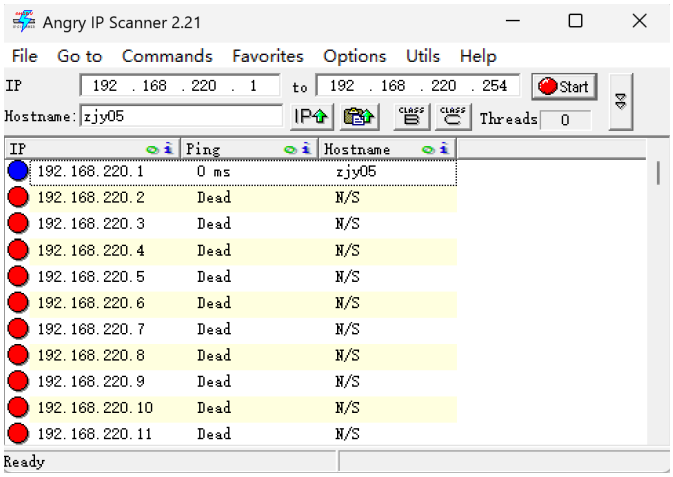
3.1　本地网络扫描结果截图及说明

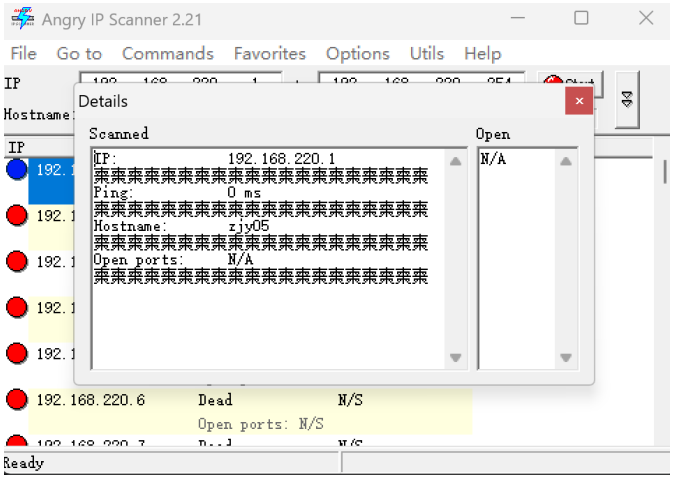
经过在命令行窗口运行 ipconfig 后得到 于是我将 ip 范围设置为 192.168.220.1-192.168.220.254



扫描结果如下，活跃主机只有 192.168.220.1

截图说明：上图展示了使用 Angry IP Scanner 对本地网络进行扫描的结果。从扫描结果可以看到，网络中有 1 个活跃主机，显示了其 IP 地址、响应状态（活跃/不活跃）以及主机名。蓝色标记的 IP 地址表示该主机处于活跃状态，可以进行进一步的端口扫描和信息收集。。





4 Nmap 命令行工具使用

4.1 主机发现技术

主机发现是网络侦察的首要步骤，旨在从大量 IP 范围中筛选出活跃或有价值的主机。Nmap 提供了多种主机发现技术，以适应不同的网络环境和安全需求。

4.1.1 基本主机发现命令

列表扫描

```
nmap -sL 192.168.1.0/24
```

说明：不发送任何数据包到目标主机，只列出指定网络中的每个主机并执行反向 DNS 解析获取主机名。适用于确认目标 IP 地址是否正确。

Ping 扫描

```
nmap -sn 192.168.1.0/24
```

说明：仅执行主机发现，不进行后续的端口扫描。默认发送 ICMP echo 请求、TCP SYN 到 443 端口、TCP ACK 到 80 端口和 ICMP 时间戳请求。适用于快速确定网络中哪些主机处于活动状态。

```
Nmap scan report for 192.168.1.229
Nmap scan report for 192.168.1.230
Nmap scan report for 192.168.1.231
Nmap scan report for 192.168.1.232
Nmap scan report for 192.168.1.233
Nmap scan report for 192.168.1.234
Nmap scan report for 192.168.1.235
Nmap scan report for 192.168.1.236
Nmap scan report for 192.168.1.237
Nmap scan report for 192.168.1.238
Nmap scan report for 192.168.1.239
Nmap scan report for 192.168.1.240
Nmap scan report for 192.168.1.241
Nmap scan report for 192.168.1.242
Nmap scan report for 192.168.1.243
Nmap scan report for 192.168.1.244
Nmap scan report for 192.168.1.245
Nmap scan report for 192.168.1.246
Nmap scan report for 192.168.1.247
Nmap scan report for 192.168.1.248
Nmap scan report for 192.168.1.249
Nmap scan report for 192.168.1.250
Nmap scan report for 192.168.1.251
Nmap scan report for 192.168.1.252
Nmap scan report for 192.168.1.253
Nmap scan report for 192.168.1.254
Nmap scan report for 192.168.1.255
Nmap done: 256 IP addresses (0 hosts up) scanned in 4.19 seconds
```

```
C:\Program Files (x86)\Nmap>nmap -sn 192.168.1.0/24
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-06 15:51 +0800
Stats: 0:02:15 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 65.43% done; ETC: 15:54 (0:01:12 remaining)
Stats: 0:02:45 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 79.59% done; ETC: 15:54 (0:00:42 remaining)
Nmap done: 256 IP addresses (0 hosts up) scanned in 207.73 seconds
```

无 Ping 扫描

```
nmap -Pn 192.168.1.100
```

说明：完全跳过主机发现阶段，对指定的每个 IP 地址执行请求的扫描功能。适用于防火墙阻止 ping 请求的情况，确保目标 IP 被扫描，无论其是否响应 ping。

```
C:\Program Files (x86)\Nmap>nmap -Pn 192.168.1.100
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-06 15:56 +0800
Stats: 0:01:26 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 42.00% done; ETC: 15:59 (0:01:57 remaining)
Stats: 0:03:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 92.50% done; ETC: 15:59 (0:00:15 remaining)
Nmap scan report for 192.168.1.100
Host is up.
All 1000 scanned ports on 192.168.1.100 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 204.00 seconds
```

4.1.2 高级主机发现技术

TCP SYN Ping

```
nmap -PS22,80,443 192.168.1.0/24
```

说明：发送带有 SYN 标志的空 TCP 数据包到指定端口。适用于绕过阻止 ICMP 但允许 TCP 连接的防火墙。

TCP ACK Ping

```
nmap -PA80 192.168.1.0/24
```

说明：发送带有 ACK 标志的 TCP 数据包。适用于绕过阻止 SYN 包的无状态防火墙。

UDP Ping

```
nmap -PU53 192.168.1.0/24
```

说明：向指定端口发送 UDP 数据包。主要优势是可绕过只筛选 TCP 的防火墙和过滤器。

```
C:\Program Files (x86)\Nmap>nmap -PS22,80,443 192.168.1.0/24
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-06 16:00 +0800
Stats: 0:00:58 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 37.43% done; ETC: 16:03 (0:01:37 remaining)
Stats: 0:02:33 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 98.96% done; ETC: 16:03 (0:00:02 remaining)
Nmap done: 256 IP addresses (0 hosts up) scanned in 157.22 seconds
```

4.2 端口扫描技术

端口扫描用于发现目标主机上开放的 TCP 和 UDP 端口。Nmap 提供了多种端口扫描技术，以适应不同的网络环境和安全需求。

4.2.1 基本端口扫描命令

默认扫描

```
nmap 192.168.220.1
```

说明：默认执行 TCP SYN 扫描，扫描常用的 1000 个 TCP 端口。这是最常用的基本扫描命令。

```
C:\Program Files (x86)\Nmap>nmap 192.168.220.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-06 16:15 +0800
Nmap scan report for 192.168.220.1
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.02 seconds
```

指定端口扫描

```
nmap -p 22,80,443 192.168.220.1
```

说明：扫描指定的端口。可以指定单个端口、多个端口或端口范围。

```
C:\Program Files (x86)\Nmap>nmap -p 22,80,443 192.168.220.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-06 16:14 +0800
Nmap scan report for 192.168.220.1
Host is up (0.00088s latency).

PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  closed http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 0.87 seconds
```

扫描所有端口

```
nmap -p- 192.168.220.1
```

说明：扫描所有 65535 个 TCP 端口。这种扫描比较耗时，但能发现隐藏在非标准端口的服务。

快速扫描

```
nmap -F 192.168.220.1
```

说明：执行快速扫描，仅扫描最常见的端口。适用于需要快速结果的场景。

```
C:\Program Files (x86)\Nmap>nmap -F 192.168.220.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-06 16:16 +0800
Nmap scan report for 192.168.220.1
Host is up (0.00078s latency).
Not shown: 97 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds
```

4.2.2 高级端口扫描技术

TCP SYN 扫描（半开放扫描）

```
nmap -sS 192.168.220.1
```

说明：这是 Nmap 的默认扫描类型，被称为" 半开放" 扫描。它发送 SYN 包但不完成完整 TCP 连接，速度快且相对隐蔽。需要 root/管理员权限。

```
C:\Program Files (x86)\Nmap>nmap -sS 192.168.220.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-06 16:18 +0800
Nmap scan report for 192.168.220.1
Host is up (0.00084s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.99 seconds
```

TCP Connect 扫描

```
nmap -sT 192.168.220.1
```

说明：使用操作系统的 connect() 系统调用建立完整 TCP 连接。当用户没有原始数据包权限时的默认 TCP 扫描类型，适合普通用户使用。

```
C:\Program Files (x86)\Nmap>nmap -sT 192.168.220.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-06 16:21 +0800
Nmap scan report for 192.168.220.1
Host is up (0.00088s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.01 seconds
```

UDP 扫描

```
nmap -sU 192.168.220.1
```

说明：检测 UDP 服务如 DNS、SNMP 和 DHCP。可与 TCP 扫描类型 (如-sS) 结合使用，同时检查两种协议。

隐蔽扫描技术

```
nmap -sN 192.168.220.1   # NULL 扫描
nmap -sF 192.168.220.1   # FIN 扫描
nmap -sX 192.168.220.1   # Xmas 扫描
```

说明：这些扫描技术利用 TCP RFC 的漏洞区分开放和关闭的端口。可以穿透某些非状态防火墙和数据包过滤路由器，比 SYN 扫描更隐蔽。

```
C:\Program Files (x86)\Nmap>nmap -sU 192.168.220.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-06 16:19 +0800
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 27.40% done; ETC: 16:19 (0:00:11 remaining)
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 75.60% done; ETC: 16:20 (0:00:11 remaining)
Nmap scan report for 192.168.220.1
Host is up (0.00033s latency).
Not shown: 992 closed udp ports (port-unreach)
PORT     STATE         SERVICE
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
500/udp  open|filtered isakmp
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 53.22 seconds
```

4.3 服务版本检测

服务版本检测可以确定端口上运行的应用程序及其版本信息。这对于安全评估和漏洞识别非常重要。

4.3.1 基本版本检测命令

启用版本检测

```
nmap -sV 192.168.220.1
```

说明：探测开放端口上运行的服务和版本。这有助于判断当前服务是否存在已知漏洞。

```
C:\Program Files (x86)\Nmap>nmap -sV 192.168.220.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-06 16:23 +0800
Nmap scan report for 192.168.220.1
Host is up (0.00065s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 7.62 seconds
```

轻量级版本检测

```
nmap -sV --version-light 192.168.220.1
```

说明： –version-intensity 2 的便捷别名。执行更快速的版本扫描，但准确性可能略低。

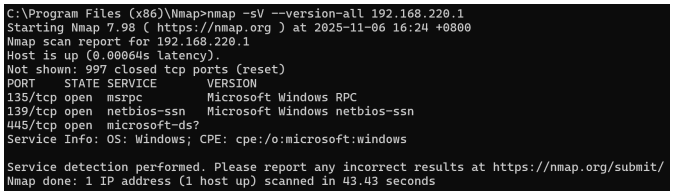
```
C:\Program Files (x86)\Nmap>nmap -sV --version-light 192.168.220.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-06 16:22 +0800
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 192.168.220.1
Host is up (0.00070s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 9.93 seconds
```

全面版本检测

```
nmap -sV --version-all 192.168.220.1
```

说明： –version-intensity 9 的别名。执行最全面、最准确的版本检测，但速度较慢。

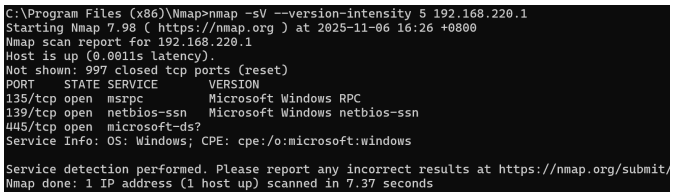


4.3.2 高级版本检测选项

设置版本扫描强度

```
nmap –sV ––version–intensity 5 192.168.220.1
```

说明：设置版本扫描强度，范围为 0-9，默认值为 7。较低的强度值适用于快速但可能不太准确的扫描，较高的强度值提供更准确的结果，但扫描时间更长。



跟踪版本扫描活动

```
nmap –sV ––version–trace 192.168.220.1
```

说明：跟踪版本扫描活动，输出详细调试信息。适用于调试版本检测问题或了解检测过程的详细信息。

4.4 操作系统识别

操作系统识别是 Nmap 最著名的特性之一，通过 TCP/IP 栈指纹识别技术，向远程主机发送一系列 TCP 和 UDP 数据包，并分析响应来确定目标系统的操作系统类型和版本。

4.4.1 基本操作系统检测命令

启用操作系统检测

```
nmap –O 192.168.220.1
```

说明：启用操作系统检测功能。Nmap 会尝试识别目标主机的操作系统类型和版本。

强制操作系统检测

```
nmap –O ––osscan–guess 192.168.220.1
```

说明：当 Nmap 无法检测到完美匹配的 OS 时，这个选项使 Nmap 更积极地猜测。Nmap 会在打印不完美匹配时告知用户，并显示每个猜测的置信度百分比。

```
C:\Program Files (x86)\Nmap>nmap -O 192.168.220.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-06 16:27 +0800
Nmap scan report for 192.168.220.1
Host is up (0.00088s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.98%E=4%D=11/6%OT=135%CT=1%CU=44347%PV=Y%DS=0%DC=L%G=Y%TM=690C5B
OS:F4%P=i686-pc-windows-windows)SEQ(SP=101%GCD=1%ISR=10D%TI=I%CI=I%II=I%SS=
OS:S%TS=A)SEQ(SP=103%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=104%GCD=
OS:1%ISR=10E%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=105%GCD=1%ISR=109%TI=I%CI=I%II
OS:=I%SS=S%TS=A)SEQ(SP=108%GCD=1%ISR=108%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=MF
OS:FD7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8ST11%O5=MFFD7NW8S
OS:T11%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN
OS:(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=
OS:AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80
OS:%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=
OS:)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%
OS:A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%
OS:DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=
OS:80%CD=Z)

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.34 seconds
```

```
C:\Program Files (x86)\Nmap>nmap -O --osscan-guess 192.168.220.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-06 16:28 +0800
Nmap scan report for 192.168.220.1
Host is up (0.0010s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
Aggressive OS guesses: Microsoft Windows 10 1607 - 11 23H2 (99%), Microsoft Windows 10 1511 (97%), Windows 11 21H2 (97%)
, Windows Server 2022 (97%), Microsoft Windows 10 1703 (96%), Microsoft Windows 10 1703 or Windows 11 21H2 (96%), Micros
oft Windows 10 1703 - 11 21H2 (95%), Microsoft Windows 11 21H2 (95%), Microsoft Windows 7 or 8.1 R1 (94%), Microsoft Win
dows 10 1809 - 21H2 (93%)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.98%E=4%D=11/6%OT=135%CT=1%CU=40465%PV=Y%DS=0%DC=L%G=Y%TM=690C5C
OS:2E%P=i686-pc-windows-windows)SEQ(SP=100%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=
OS:S%TS=A)SEQ(SP=102%GCD=1%ISR=107%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=104%GCD=
OS:1%ISR=108%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=104%GCD=1%ISR=10D%TI=I%CI=I%II
OS:=I%SS=S%TS=A)OPS(O1=MFFD7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFF
OS:D7NW8ST11%O5=MFFD7NW8ST11%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FF
OS:FF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y
OS:%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD
OS:=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%
OS:S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(
OS:R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F
OS:=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G
OS:%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 0 hops
```

4.4.2 高级操作系统检测选项

限制操作系统检测

```
nmap –O ––osscan–limit 192.168.220.1
```

说明：限制 OS 检测仅针对有希望的目标。该选项使 Nmap 只对至少有一个开放端口和一个关闭 TCP 端口的主机进行 OS 检测，可以节省大量时间。

```
C:\Program Files (x86)\Nmap>nmap -O --osscan-limit 192.168.220.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-06 16:30 +0800
Nmap scan report for 192.168.220.1
Host is up (0.00087s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.98%E=4%D=11/6%OT=135%CT=1%CU=36537%PV=Y%DS=0%DC=L%G=Y%TM=690C5C
OS:B9%P=i686-pc-windows-windows)SEQ(SP=102%GCD=1%ISR=10A%TI=I%CI=I%II=I%SS=
OS:S%TS=A)SEQ(SP=104%GCD=1%ISR=10A%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=F9%GCD=1
OS:%ISR=100%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=FC%GCD=1%ISR=10D%TI=I%CI=I%II=I
OS:%SS=S%TS=A)OPS(O1=MFFD7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7
OS:NW8ST11%O5=MFFD7NW8ST11%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF
OS:%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%D
OS:F=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0
OS:%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=
OS:A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=
OS:Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=A
OS:R%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%R
OS:UD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.13 seconds
```

设置操作系统检测尝试次数

```
nmap –O ––max–os–tries 3 192.168.220.1
```

说明：设置对目标进行 OS 检测尝试的最大次数。指定较低的值可加快 Nmap 速度，但可能会错过可能识别 OS 的重试机会。

```
C:\Program Files (x86)\Nmap>nmap -O --max-os-tries 3 192.168.220.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-06 16:31 +0800
Nmap scan report for 192.168.220.1
Host is up (0.00086s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.98%E=4%D=11/6%OT=135%CT=1%CU=33609%PV=Y%DS=0%DC=L%G=Y%TM=690C5C
OS:F4%P=i686-pc-windows-windows)SEQ(SP=105%GCD=1%ISR=10A%TI=I%CI=I%II=I%SS=
OS:S%TS=A)SEQ(SP=105%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=107%GCD=
OS:1%ISR=10A%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=MFFD7NW8ST11%O2=MFFD7NW8ST11%O
OS:3=MFFD7NW8NNT11%O4=MFFD7NW8ST11%O5=MFFD7NW8ST11%O6=MFFD7ST11)WIN(W1=FFFF
OS:%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD
OS:7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%
OS:W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=
OS:)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=
OS:S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF
OS:=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=
OS:G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.80 seconds
```

4.5 综合扫描技术

综合扫描技术结合了多种扫描功能，提供更全面的目标信息。

4.5.1 基本综合扫描命令

全面系统检测

```
nmap -A 192.168.220.1
```

说明：启用操作系统检测、版本检测、脚本扫描和 traceroute。这是一个非常有用的综合扫描选项，提供丰富的目标信息。

```
C:\Program Files (x86)\Nmap>nmap -A 192.168.220.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-06 16:32 +0800
Nmap scan report for 192.168.220.1
Host is up (0.00061s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.98%E=4%D=11/6%OT=135%CT=1%CU=37773%PV=Y%DS=0%DC=L%G=Y%TM=690C5D
OS:5A%P=i686-pc-windows-windows)SEQ(SP=100%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=
OS:S%TS=A)SEQ(SP=101%GCD=1%ISR=104%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=101%GCD=
OS:1%ISR=108%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=102%GCD=1%ISR=104%TI=I%CI=I%II
OS:=I%SS=S%TS=A)SEQ(SP=107%GCD=2%ISR=109%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=MF
OS:FD7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8ST11%O5=MFFD7NW8S
OS:T11%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN
OS:(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=
OS:AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80
OS:%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=
OS:)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%
OS:A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%
OS:DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=
OS:80%CD=Z)

Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
| smb2-time:
|   date: 2025-11-06T08:33:17
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 36.51 seconds
```

详细扫描

```
nmap -v -A 192.168.220.1
```

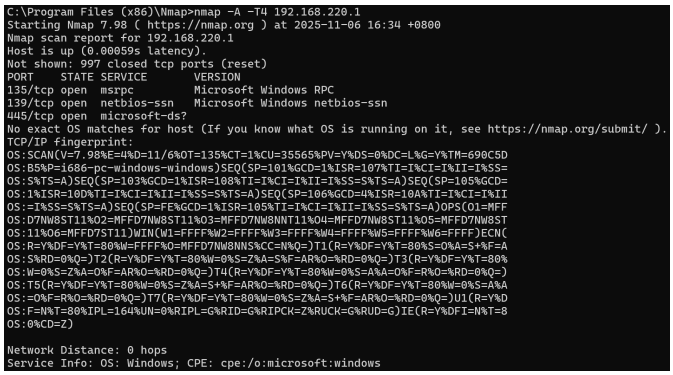
说明：启用详细模式和全面系统检测。详细模式会提供更多的扫描信息，包括进度和发现的细节。

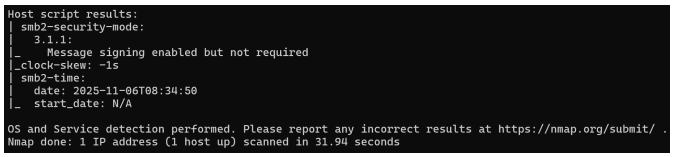
4.5.2 高级综合扫描技术

综合扫描并控制速度

```
nmap –A –T4 192.168.220.1
```

说明：执行全面系统检测，并设置时序模板为 4(Aggressive)。这可以加快扫描速度，但可能会更容易被目标检测到。





5 实验总结

通过本次实验，我掌握了 Angry IP Scanner 和 Nmap 两款网络扫描工具的基本使用方法。这些工具可以帮助网络管理员发现网络中的设备、检测开放端口和服务，对网络安全评估和管理具有重要意义。

在实验过程中，我了解到：

1. Angry IP Scanner 操作简单，界面友好，适合快速扫描局域网，能够直观地显示网络中的活跃主机和开放端口
2. Nmap 功能强大，命令选项丰富，可以进行更深入的网络探测，包括服务版本检测、操作系统识别等高级功能
3. 网络扫描可以发现潜在的安全隐患，如不必要的开放端口，这对于网络安全管理至关重要
4. 这些工具应当在合法授权的情况下使用，避免对他人网络造成干扰