

# 端口扫描实验

## 一【实验目标】

- 掌握端口扫描技术基本原理
- 学会使用 Superscan 对目标主机的端口进行扫描。

## 二【实验环境】

- Windows 10 操作系统
- superscan4.exe

## 三【实验原理】

端口扫描，顾名思义，就是逐个对一段端口或指定的端口进行扫描。通过扫描结果可以知道一台计算机上都提供了哪些服务，然后就可以通过所提供的这些服务的已知漏洞就可进行攻击。其原理是当一个主机向远端一个服务器的某一个端口提出建立一个连接的请求，如果对方有此项服务，就会应答，如果对方未安装此项服务时，即使你向相应的端口发出请求，对方仍无应答，利用这个原理，如果对所有熟知端口或自己选定的某个范围内的熟知端口分别建立连接，并记录下远端服务器所给予的应答，通过查看一记录就可以知道目标服务器上安装了哪些服务，这就是端口扫描，通过端口扫描，就可以搜集到很多关于目标主机的各种很有参考价值的信息。例如，对方是否提供 FTP 服务、WWW 服务或其它服务。

## 四【实验步骤】

实验具体操作步骤如下：

1. 进入系统，输入密码“Admin123456”，如图 1 所示。

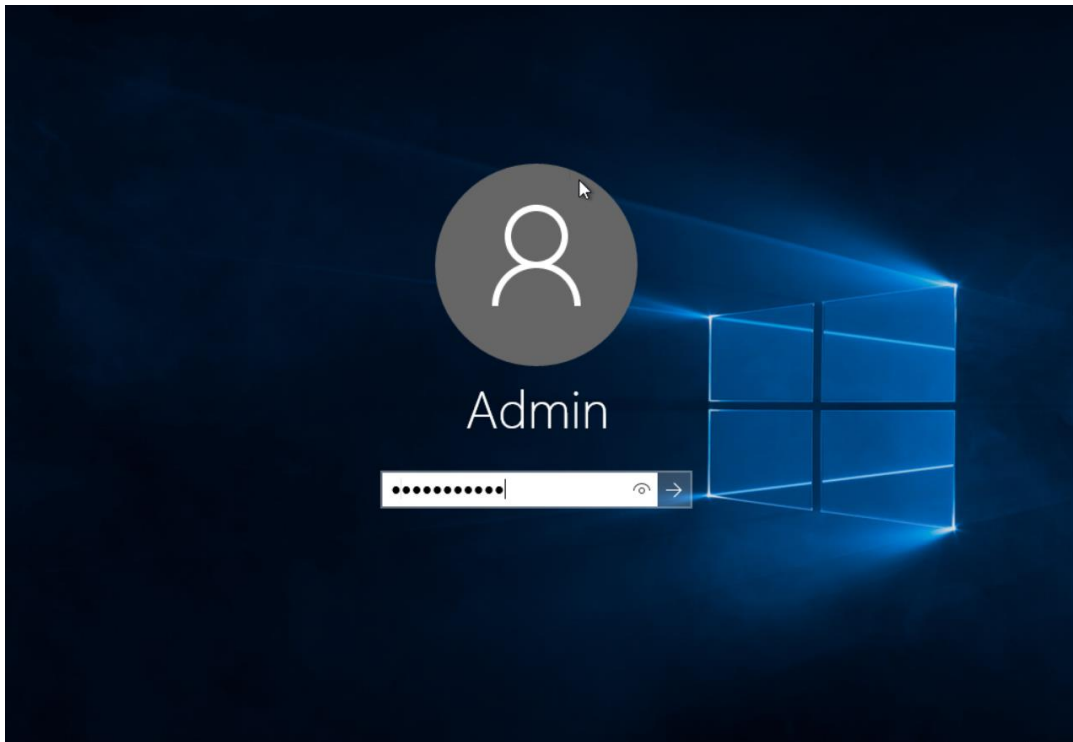


图 1

2. 点击【文件资源管理器】，进入 C 盘【tools】文件夹。如图 2 所示。

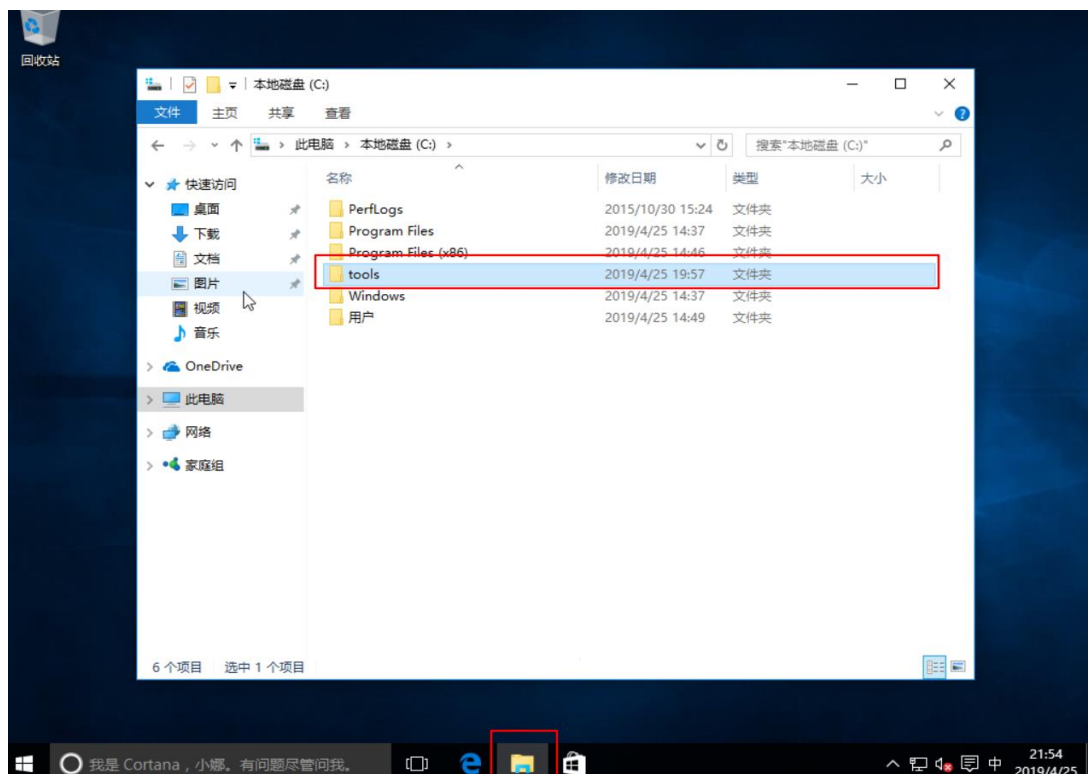


图 2

3. 进入【网络扫描】文件夹，右键选择【superscan4】，选择以【管理员身份运行】。如图 3 所示。

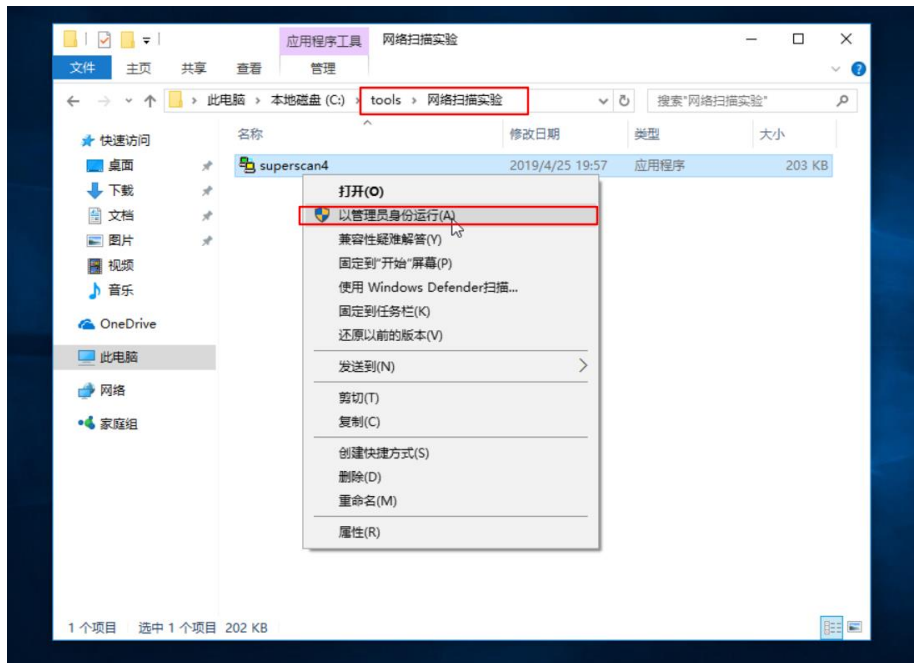


图 3

4. Superscan 主界面如图 4 所示。

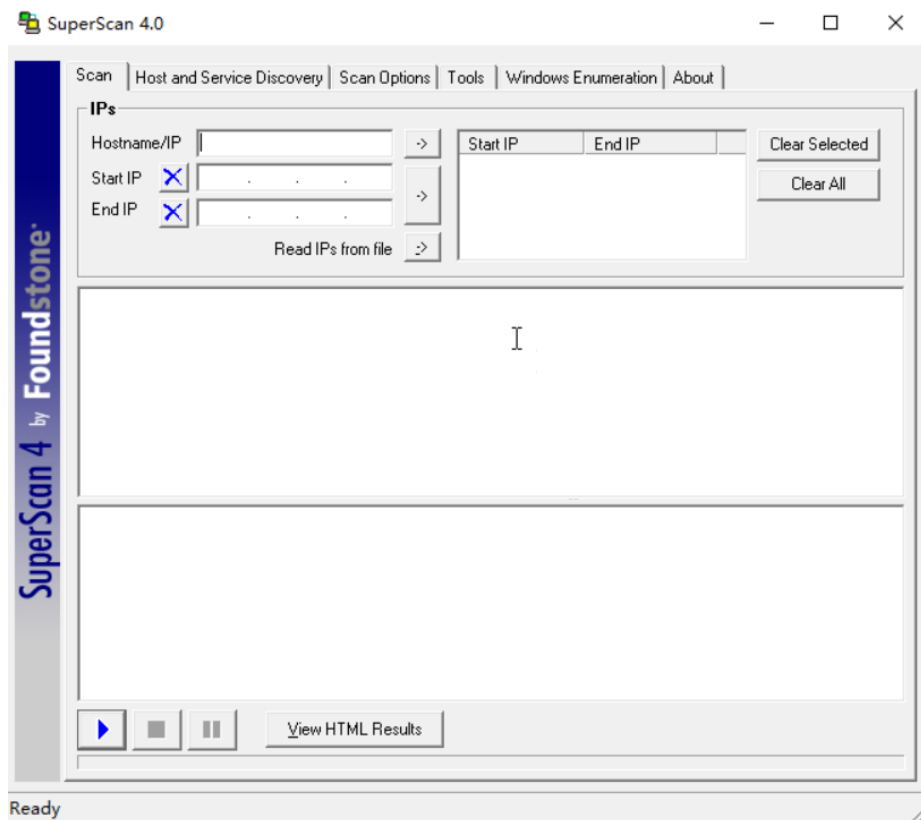


图 4

5. 基本参数设置。Superscan 界面主要包括的选项卡有：**【Scan】**（扫描）选项卡：用来进行端口扫描；**【Host and Service Discovery】**（主机和服务扫描设置）选项卡：用来设置主机和服务选项，包括要扫描的端口类型和端口列

表；【Scan Options】（扫描选项） 选项卡：设置扫描任务选项；【Tools】（工具）选项卡：提供的特殊扫描工具，可以借助这些工具对特殊服务进行扫描；【Windows Enumeration】（Windows 枚举） 选项卡：对目标主机的一些主机信息进行扫描。要进行扫描首先要对扫描任务的选项进行设置，主要是设置【Host and Service Discovery】选项卡和【Scan Options】选项卡。（为方便阅读，下面使用中文）

6. 点击“开始”，输入“cmd”，点击“命令提示符”，如图 5 所示。

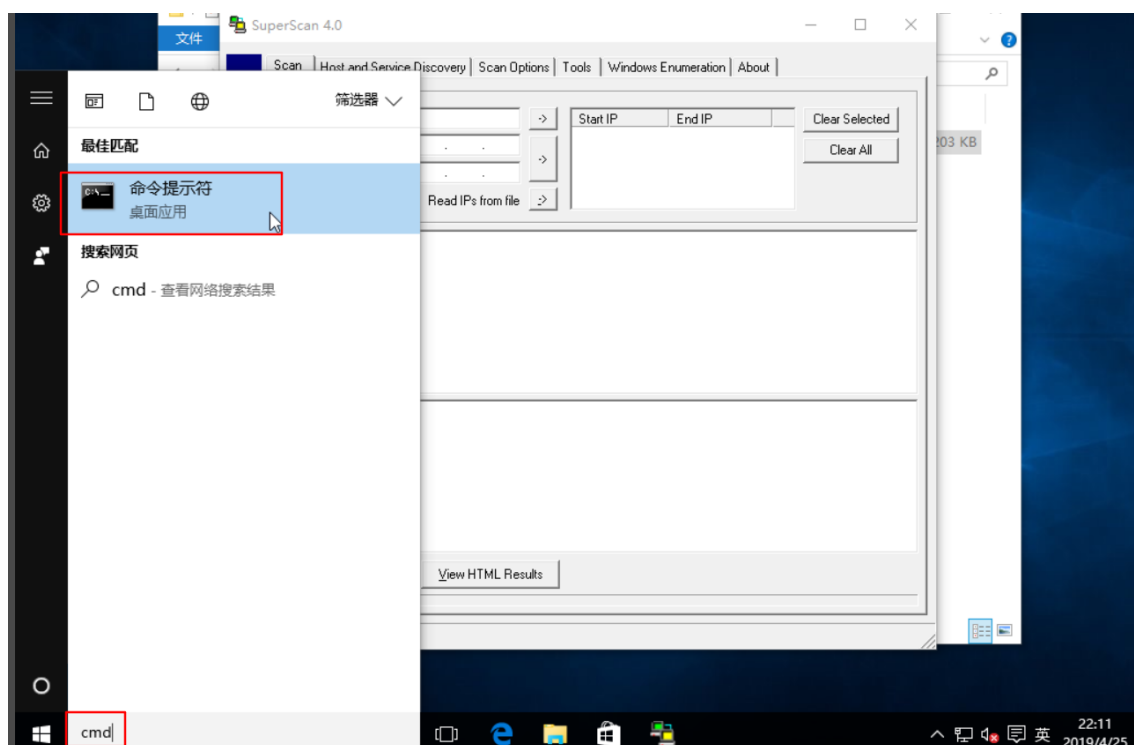


图 5

7. 输入“ipconfig”命令查看本机 IP 地址。如图 6 所示。



图 6

8. 在【主机和服务扫描设置】选项卡中，在【UDP 端口扫描】和【TCP 端口扫描】两栏中可以分别设置要扫描的 UDP 端口或 TCP 端口列表，可以自己添加要扫描的端口号，同样也可以从文本类型的端口列表文件中导入。在【超时设置】文本框中要设置扫描超时等待时间；其它按默认即可。如图 7 所示。

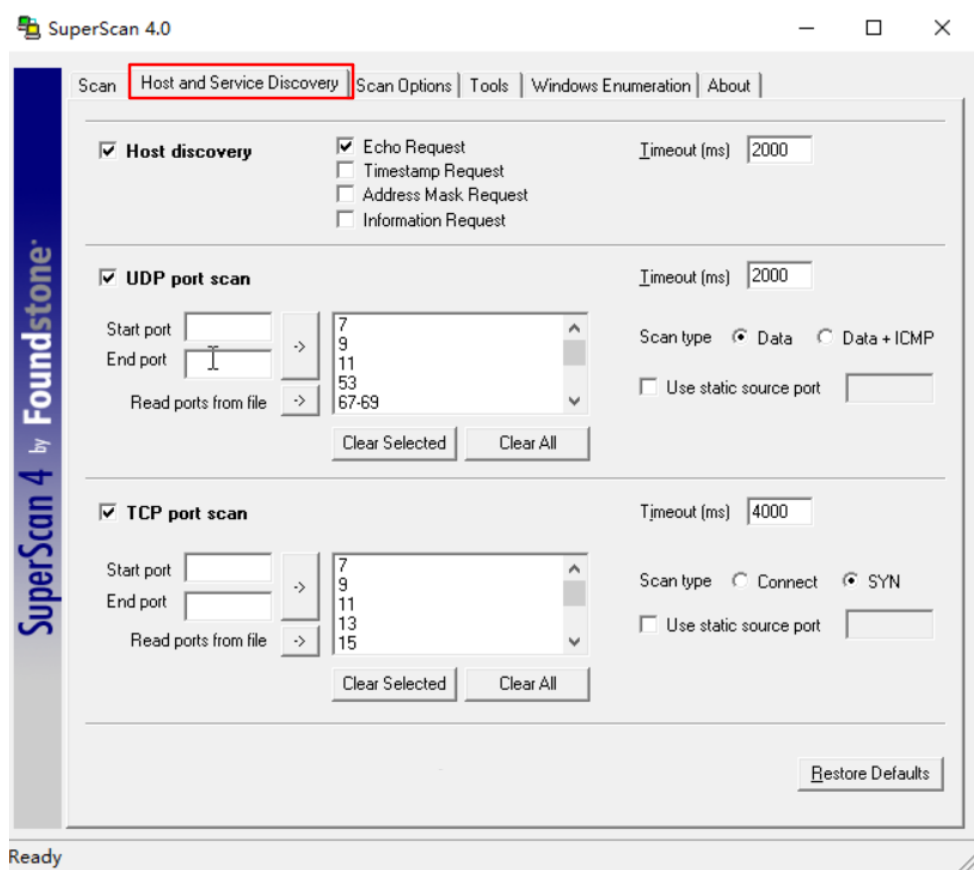


图 7

9. 在【扫描选项】选项卡中，可以设置扫描时检测开放主机或服务的次数，解析主机名的次数，获取 TCP 或者 UDP 标志的超时，以及扫描的速度。一般也可按默认设置即可。
10. 设置【扫描】选项卡。如果是对非连续 IP 地址的目标主机进行扫描，则可以在【主机名/IP】文本框中输入目标主机的主机名，或 IP 地址，然后单击【->】按钮，把要扫描的目标主机添加到中间部分的列表框中；若要对连续 IP 地址的目标主机进行扫描，则在开始 IP 和结束 IP 的文本框中输入开始和结束的 IP 地址，然后单击【->】按钮，把要扫描的连续 IP 主机添加到中间部分的列表框中。然后单击对话框底部左边的开始按钮即开始扫描，扫描的结果在下面的列表框中显示。本实验中设置主机，开始 IP 和结束 IP 均为靶机的 IP 地址“192.168.48.246”（实验时以实际 IP 为准）。如图 8 所示。

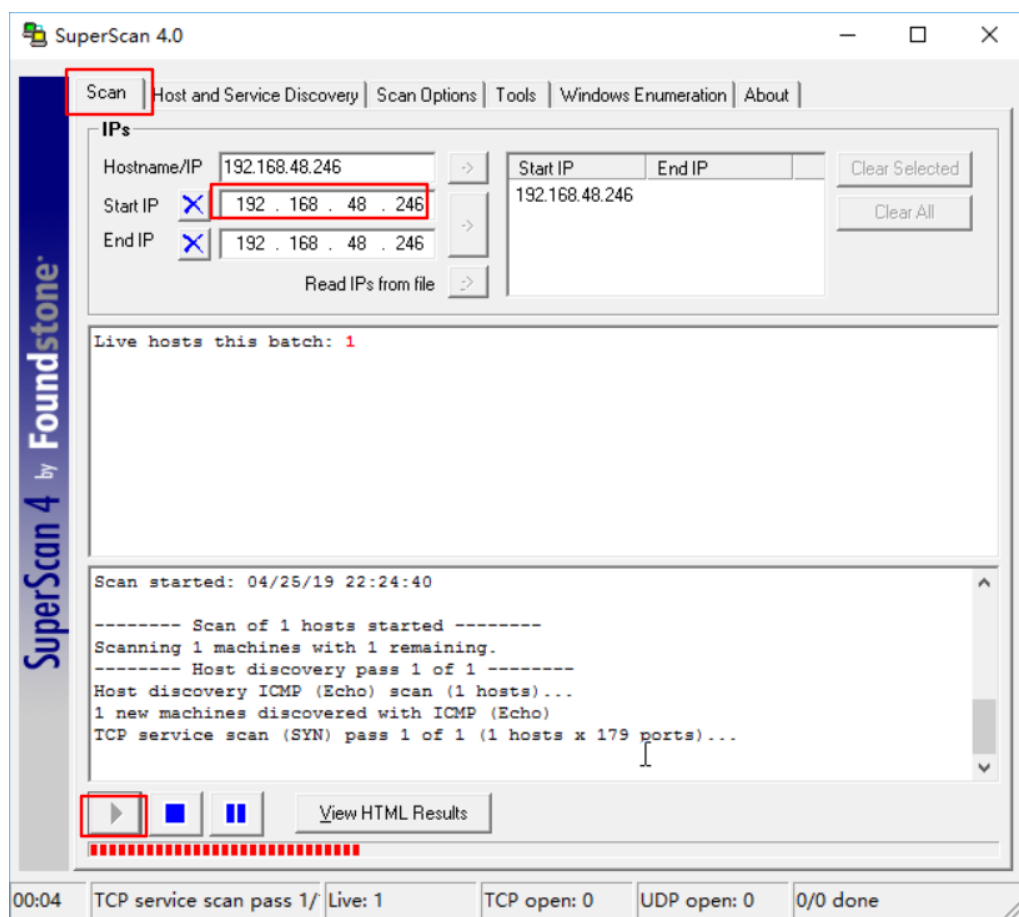


图 8

11. 查看扫描结果。从扫描结果可以看出目标主机的主机名、开放端口等信息。最后单击【查看 HTML 结果】按钮。如图 9 所示。

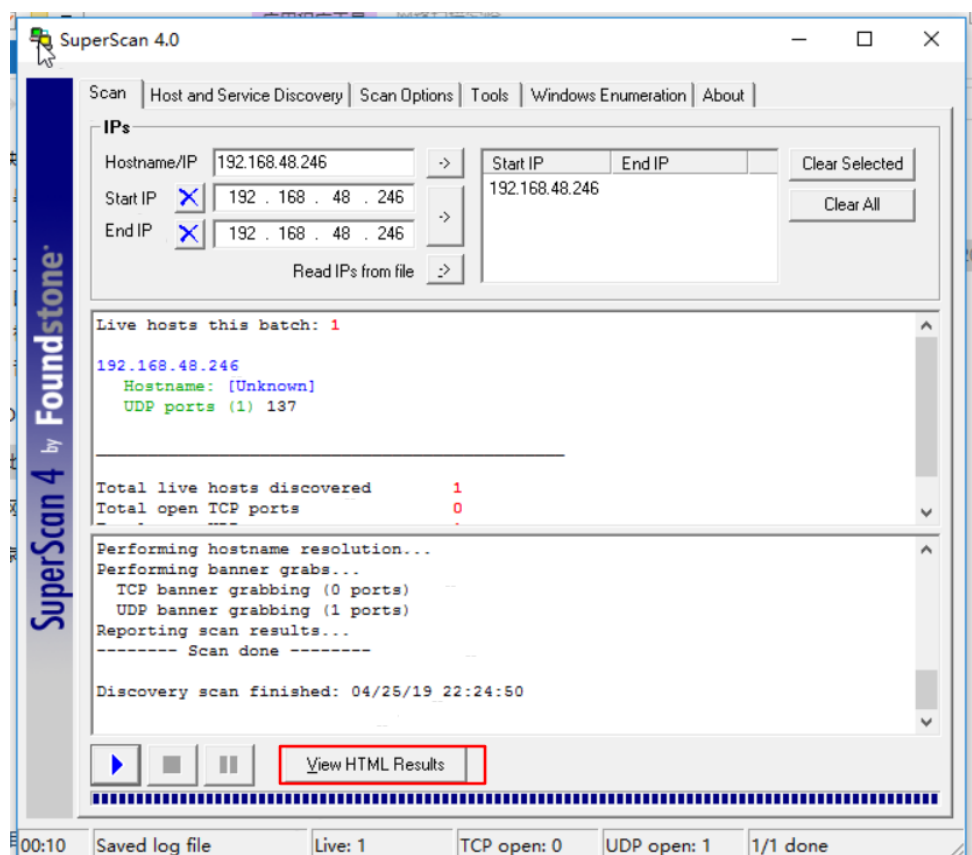


图 9

12. 实验结果以网页形式显示，可以更清楚地看出扫描后的结果。结果中显示了目标主机上的主机名、MAC 地址、用户账户和所开放的端口。如图 10 所示。

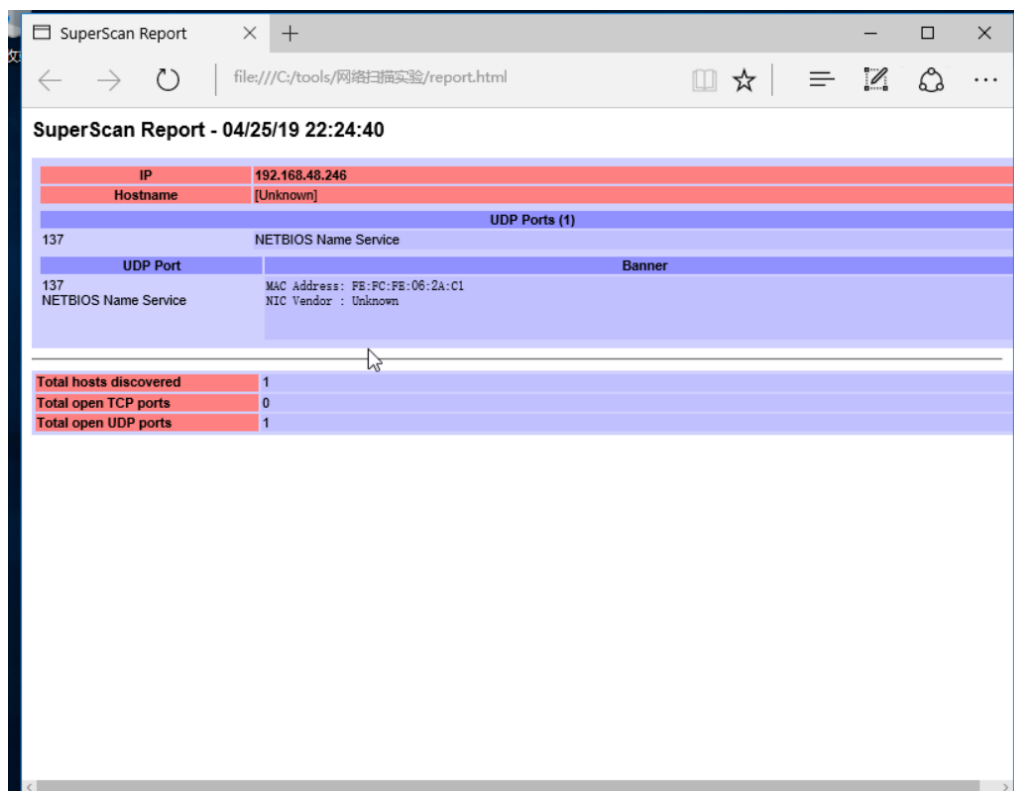


图 10

13. 工具选项卡中提供的工具可以对目标主机进行各种测试，还可以对网站进行测试。首先在【主机名/IP/URL】文本框中输入要测试的主机或网站的主机名，或 IP 地址，或者 URL 网址，然后再单击窗口中的相应工具按钮，进行对应的测试，如查找目标主机名、进行 Ping 测试操作、ICMP 跟踪、路由跟踪、HTTP 头请求查询等。如果要进行 Whois 测试，则需在【默认 Whois 服务器】文本框中输入 Whois 服务器地址。本实验中主机名输入本机 IP 地址：“192.168.48.246”（以实际 IP 为准），默认 whois 服务器设置为：“whois.networksolutions.com”测试结果会在列表中显示。如图 11 所示。

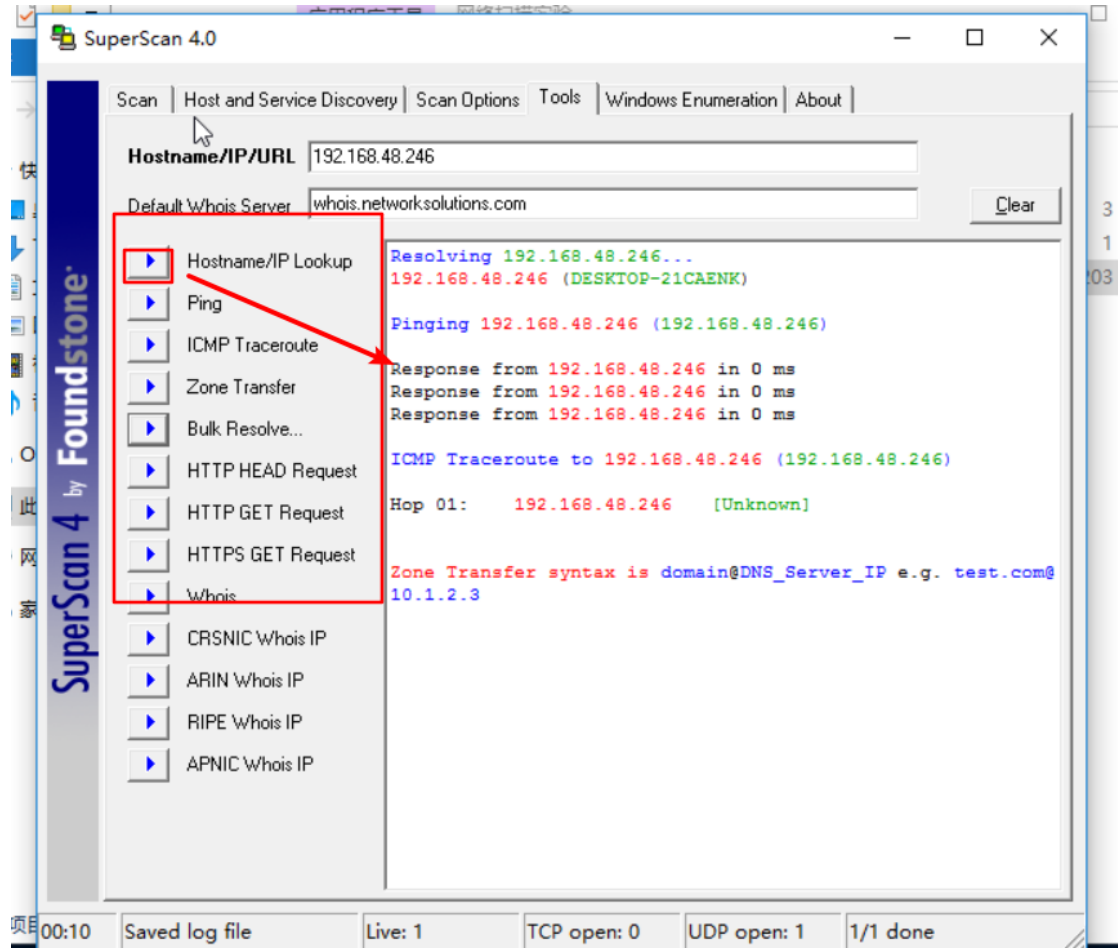


图 11

14. 【Windows 枚举】选项卡是对目标主机的一些 Windows 信息进行扫描，检测目标主机的 NetBIOS 主机名、MAC 地址、用户/组信息、共享信息等。首先在对对话框顶部的【主机名/IP/URL】文本框中输入主机名、IP 地址或网站 URL，然后在左边窗格中选择要检测的项目，然后再单击【Enumerate】按钮即在列表框中显示所选测试项目的结果。本实验中输入主机名，点击【Enumerate】，如图 12 所示。

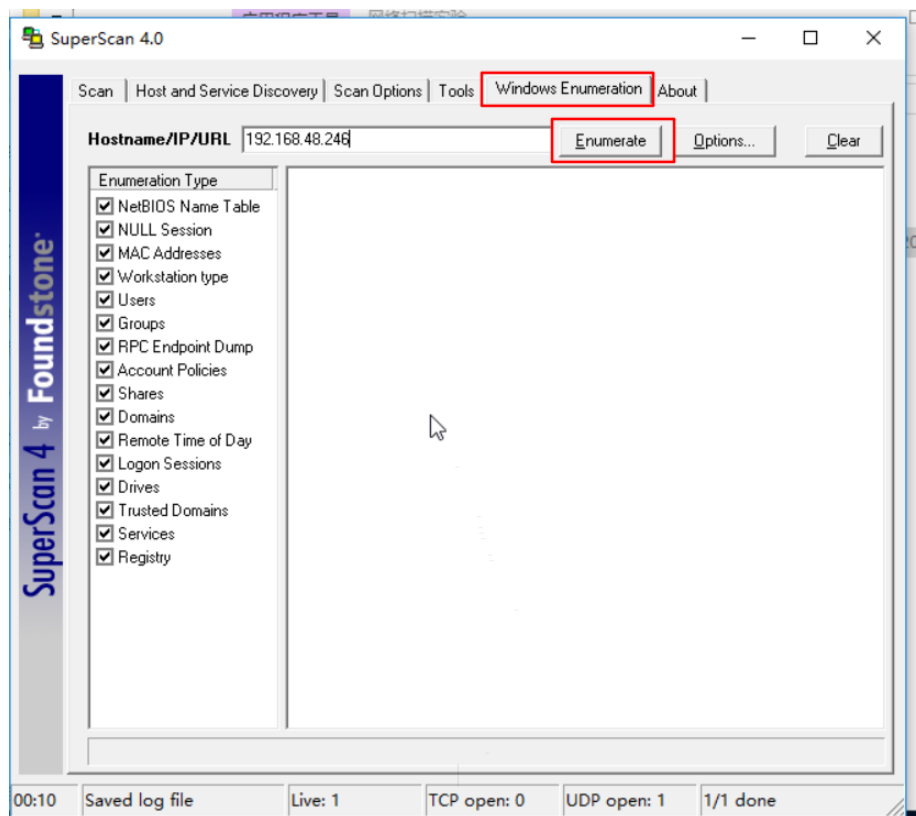


图 12

15. 实验结果如图 13 所示。

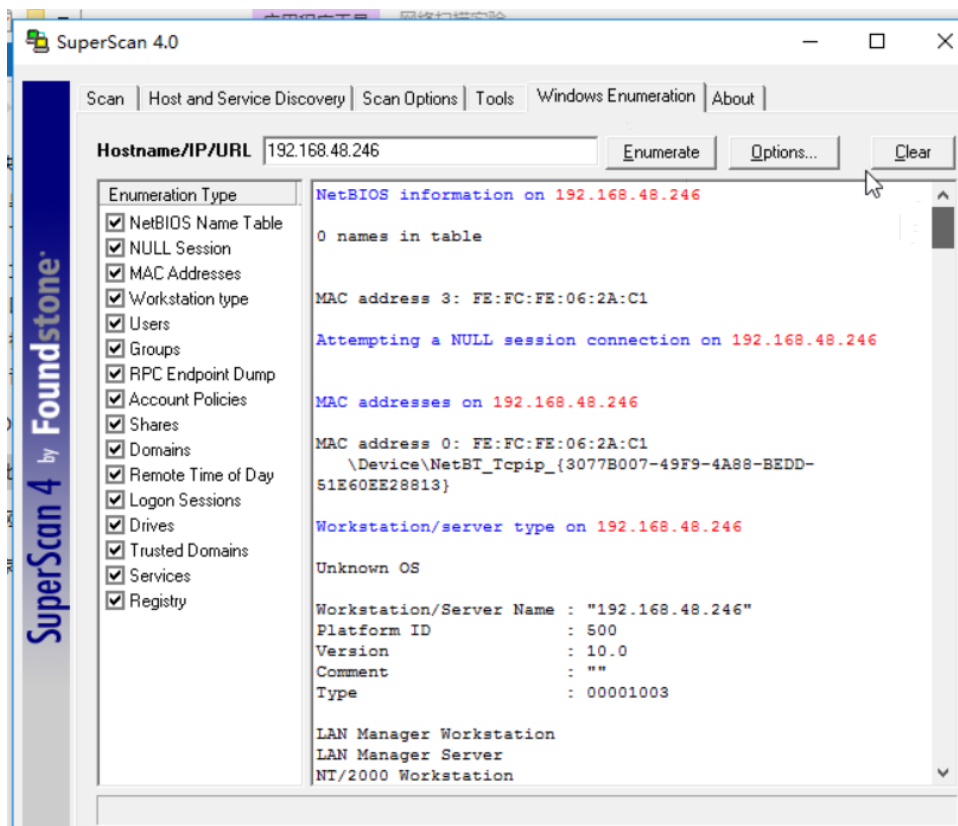


图 13

## 五【实验思考】

- 扫描不同网段，并设置不同参数，全面了解网络扫描的原理。