陕西科技大学

# 《计算机网络安全》实验报告


## 实验三：网络扫描与监听

学　　生：

学　　院：电子信息与人工智能学院

专　　业：网络工程

指导教师：张楠

**2022 年 6 月 2 日**

# 实验三 网络扫描与监听

班级：_____ _____ _____

## 实验预习报告

## 一、实验目的

1、掌握网络扫描的方法

2、通过网络扫描发现漏洞的存在

3、通过网络扫描获取对方的相关信息

## 二、实验要求

使用相关的命令和工具完成网络扫描，掌握主机漏洞扫描、端口扫描操作系统类型扫描和扫描软件的使用方法。

通过网络扫描发现对方可能存在的漏洞并尝试发现对方的信息。

## 三、实验原理

1、ARP（地址解析协议）扫描是通过发送 ARP 请求来获取局域网中活动主机的 MAC 地址和 IP 地址的技术。它可以帮助确定局域网上哪些 IP 地址被分配给了实际的主机设备。

nmap 使用 ARP 扫描时，会发送 ARP 请求包到局域网上的广播地址，并监听响应以获取活动主机的 MAC 地址和 IP 地址。

2、端口扫描是用于确定目标主机上哪些端口是开放的或关闭的。通过检查主机上不同端口的响应情况，可以获取目标主机上运行的服务和应用程序的信息。

nmap 使用不同的扫描技术（如 TCP 扫描、UDP 扫描、SYN 扫描等）发送特定类型的数据包到目标主机的不同端口，并根据响应情况来确定端口的状态。

3、主机类型扫描用于识别目标主机的操作系统或设备类型。不同的操作系统或设备在网络上的行为和响应方式可能会有所不同，因此可以通过分析目标主机的响应来猜测其类型。

nmap 通过发送特定的网络数据包到目标主机，并根据响应中的特征信息（如

TCP 标志位、IP 字段等）来推断目标主机的操作系统类型或设备类型。

4、主机漏洞扫描是用于检测目标主机上存在的已知安全漏洞或弱点。它可以帮助发现系统中可能存在的安全风险，并及时采取措施进行修复和加固。

nmap 通过使用特定的漏洞扫描脚本或插件，对目标主机进行漏洞扫描。这些脚本或插件利用已知的漏洞或弱点进行探测，并返回相应的扫描结果。

## 四、实验预习内容

1、ARP 扫描可以用来发现活动主机，通过 ARP 扫描，可以确定局域网上哪些 IP 地址被实际主机设备使用，帮助网络管理员了解网络中的活动主机情况。同时也可以实现网络映射和拓扑发现：通过获取 MAC 地址和 IP 地址的对应关系，可以绘制网络拓扑图和识别网络中的设备。

2、端口扫描一般用作安全评估，通过端口扫描，可以确定目标主机上开放的端口和运行的服务，帮助进行安全评估和漏洞扫描。可以识别潜在的安全风险和暴露的服务。

3、主机类型扫描一般永远也网络侦察，即：通过识别目标主机的操作系统或设备类型，可以获取有关网络中的设备和系统的信息。这有助于进行网络侦察和了解目标网络的特征和架构。

4、主机漏洞扫描在漏洞识别方面具有重要作用，主机漏洞扫描可以识别目标主机上已知的安全漏洞或弱点。这有助于发现系统中存在的安全风险，并及时采取修复措施来保护系统免受攻击。安全加固：通过发现漏洞，可以帮助管理员采取相应的安全加固措施，修复已知的漏洞或配置弱点，提高系统的安全性。

5、总的来说，这些扫描方法可以帮助网络管理员了解网络拓扑、评估安全风险、进行安全审计和优化防护措施，提高网络的安全性和可靠性。

# 实验三 网络扫描与监听

班级：_____ _____ _____

## 实验报告

## 一、实验目的

1、掌握网络扫描的方法

2、通过网络扫描发现漏洞的存在

3、通过网络扫描获取对方的相关信息

## 二、实验要求

使用相关的命令和工具完成网络扫描，掌握主机漏洞扫描、端口扫描操作系统类型扫描和扫描软件的使用方法。

通过网络扫描发现对方可能存在的漏洞并尝试发现对方的信息。

## 三、实验原理

1、ARP（地址解析协议）扫描是通过发送 ARP 请求来获取局域网中活动主机的 MAC 地址和 IP 地址的技术。它可以帮助确定局域网上哪些 IP 地址被分配给了实际的主机设备。

nmap 使用 ARP 扫描时，会发送 ARP 请求包到局域网上的广播地址，并监听响应以获取活动主机的 MAC 地址和 IP 地址。

2、端口扫描是用于确定目标主机上哪些端口是开放的或关闭的。通过检查主机上不同端口的响应情况，可以获取目标主机上运行的服务和应用程序的信息。

nmap 使用不同的扫描技术（如 TCP 扫描、UDP 扫描、SYN 扫描等）发送特定类型的数据包到目标主机的不同端口，并根据响应情况来确定端口的状态。

3、主机类型扫描用于识别目标主机的操作系统或设备类型。不同的操作系统或设备在网络上的行为和响应方式可能会有所不同，因此可以通过分析目标主机的响应来猜测其类型。

nmap 通过发送特定的网络数据包到目标主机，并根据响应中的特征信息（如

TCP 标志位、IP 字段等）来推断目标主机的操作系统类型或设备类型。

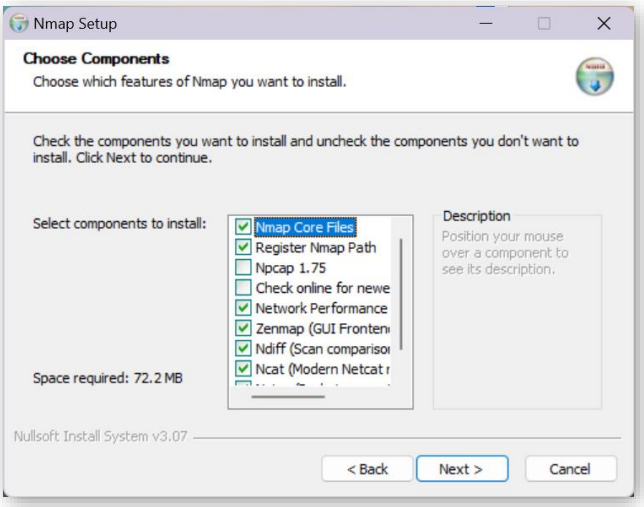
4、主机漏洞扫描是用于检测目标主机上存在的已知安全漏洞或弱点。它可以帮助发现系统中可能存在的安全风险，并及时采取措施进行修复和加固。

nmap 通过使用特定的漏洞扫描脚本或插件，对目标主机进行漏洞扫描。这些脚本或插件利用已知的漏洞或弱点进行探测，并返回相应的扫描结果。

## 四、实验内容

1、下载、安装 Nmap 到 Windows 主机上

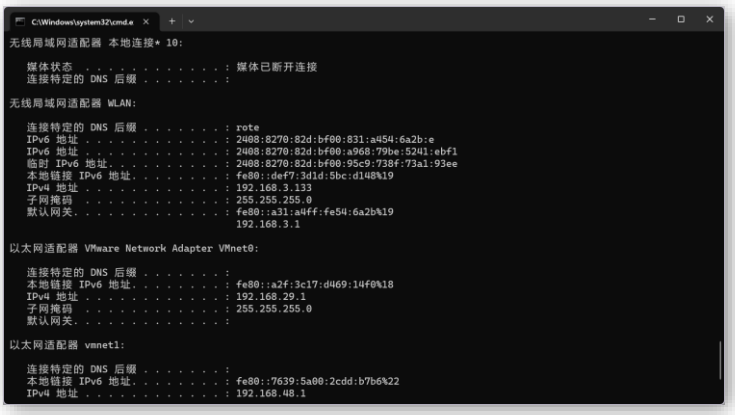
打开 Nmap 官网 https://nmap.org/download#windows，下载适用于 Windows 系统的 nmap 安装包，根据提示完成 nmap 及其插件的安装。



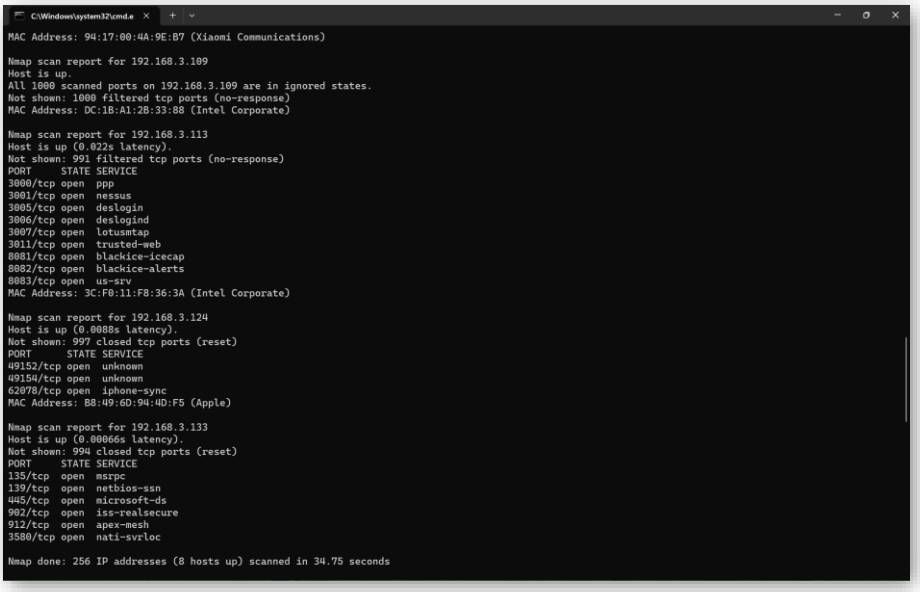

安装 Nmap

2、使用 Nmap 进行 arp 扫描，探明当前网络中存活的主机

先行使用 ipconfig 查看本机 IP 段，在该网段内进行扫描：



可以看到，当前主机位于 192.168.3.0/24 网络当中，对这个网段进行 arp 扫描：



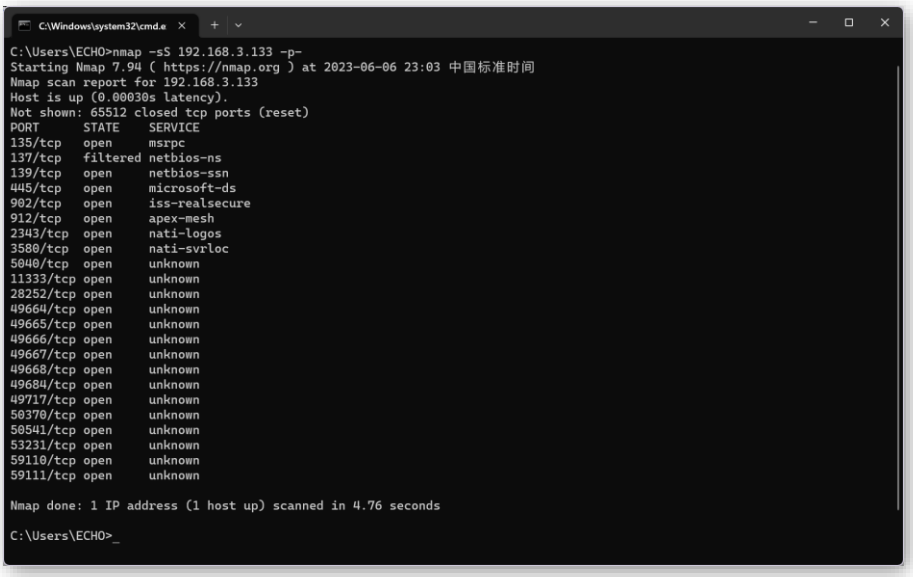

扫描结果：一共扫描到了 8 台设备。

3、进行端口扫描

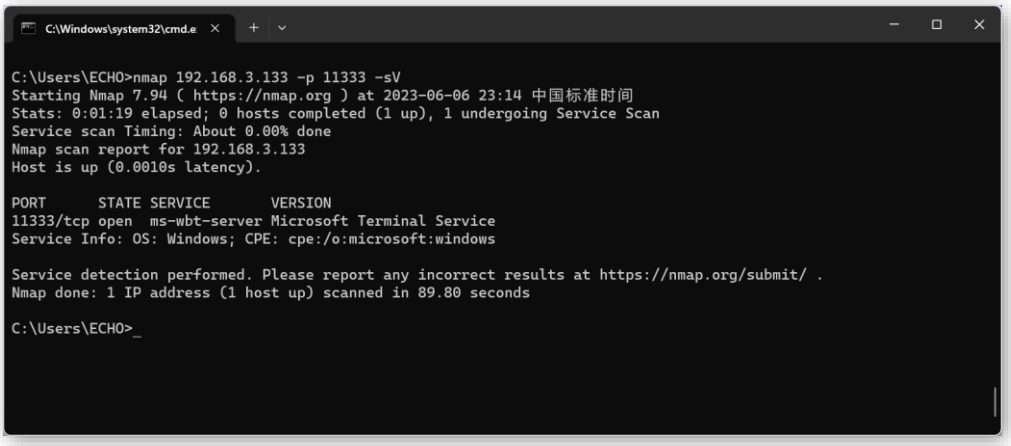
根据 arp 扫描的结果，知道了网络当中存在哪些主机，现可以对主机发起端口扫描，查看开放了哪些端口。

为了防止影响到局域网内别的主机同时能够验证扫描的结果，这里以本机（192.168.3.133）作为端口扫描的对象。

开始扫描：

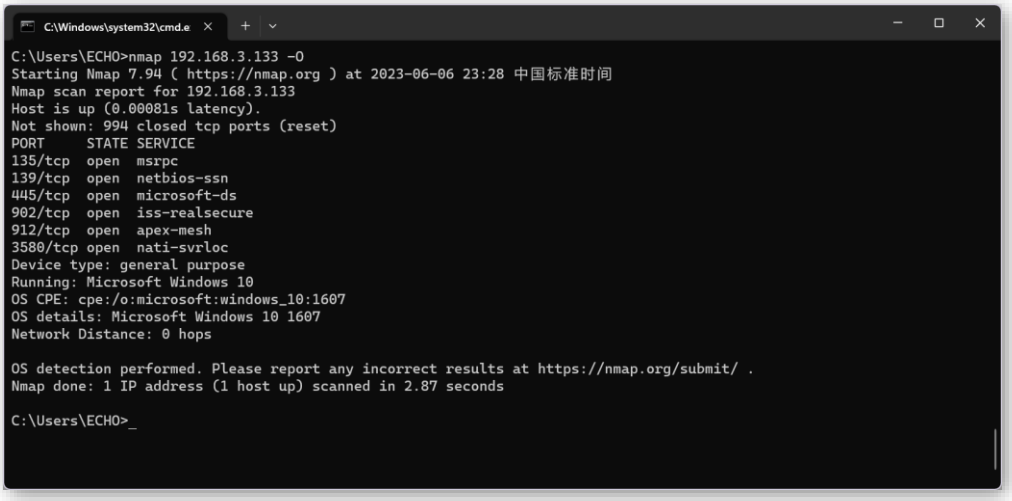


使用 nmap 对本机进行半连接 Tcp 扫描，打开的端口如上。其中，11333 是本机的 RDP 远控端口，使用 nmap 对这个端口上面的服务进行扫描：




通过端口扫描发现，该端口运行了微软的控制台服务，即 Remote Desktop Service，结果准确。

4、使用 nmap 进行主机类型扫描，扫描本机：

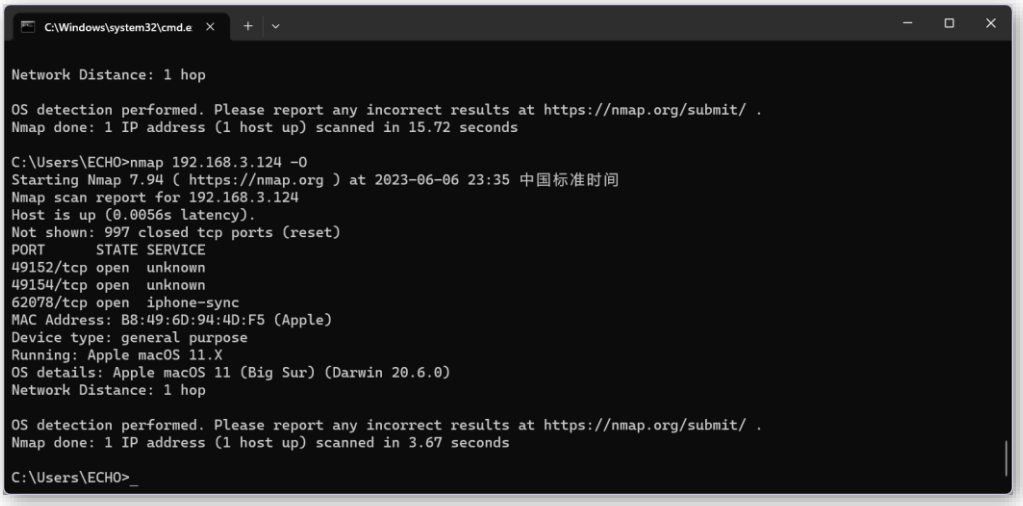



nmap 扫描到本机为 Windows10 1607，事实上，本机运行 Windows11 22H2，这说明微软对于 Windows11 中的某些功能是从早期稳定的 Windows10 当中搬过来的。

扫描局域网内的 Apple iOS 设备:

nmap 192.168.3.124 -O

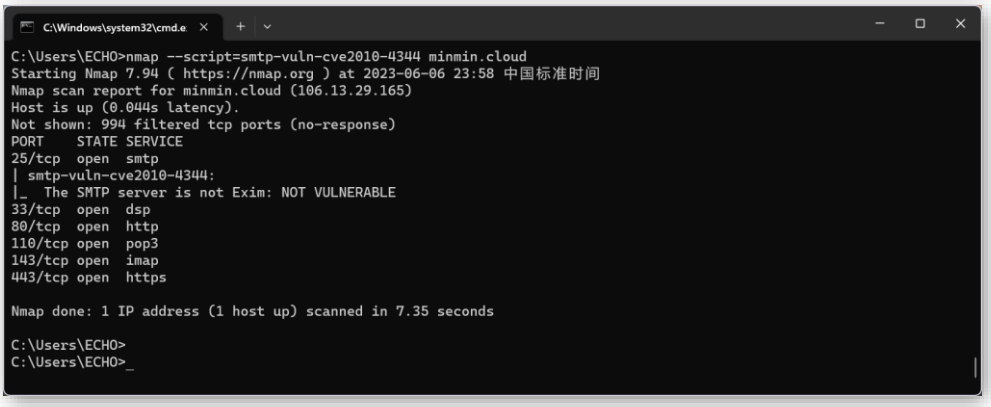
结果如下：




可以看到，nmap 扫描到了系统详情为 Apple macOS 11 （Big Sur）（Darwin 20.6.0），苹果在其系统上采取了类似微软的做法，即：从别的系统移植网络服务套件到其其它产品上，造成平台识别的不准确，事实上，这台设备运行的是 iOS 而非 macOS。

5、使用漏洞扫描查看服务器是否存在相关漏洞

尝试使用漏洞扫描查找编号为 smtp-vuln-cve2010-4344 的漏洞，对邮件服务器 minmin.cloud 进行漏扫：




看到，该服务器所运行的 SMTP 并非 Exim，所以漏扫没有扫描这个漏洞。

如果服务器所运行的操作系统、驱动程序或者是应用程序存在安全漏洞，其特征符合所要扫描的漏洞，则 Nmap 将会呈现出其具有的问题，方便进行排查，为系统的安全性提供保障。

## 五、实验结论

1、Arp 扫描广泛存在于网络当中，使用 Arp 扫描可以知道网络中存在哪些主机，进而可以准备进行具体的端口扫描。

2、端口扫描可以基本确定目标主机运行并开放了哪些端口，以及端口所运行的程序，这里可以发现并关闭不必要的端口，为系统安全提供保障，同时也可以针对这些端口进行漏扫，发现不足并及时修补。

3、主机扫描可以用于分析网络中存在的主机及其类型，进而可以根据其操作系统的不同执行特定的漏洞扫描。

4、漏洞扫描有助于及时解决已知问题，避免被利用产生损失，通过漏扫发现存在的安全隐患并及时排查，提高系统安全性。

5、Nmap 是一款十分强大的网络扫描、分析软件，可以使用它完成网络中的分析、维护工作。