|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 姓名： 崔文帅 | | 学号：2025060163 | 专业年级：2020 | 班级： 网三 |
| 分组： | | 实验室：402 | 指导教师：郭念 | 实验日期：2023-03-31 |
| **实验的准备阶段**  **(指导教师填写)** | **课程名称** | **网络协议分析与攻防技术** | | |
| **实验名称** | 实验六 网络扫描技术 | | |
| **实验目的** | 1. 掌握TCP全连接端口扫描原理。 2. 掌握SYN端口扫描原理。 | | |
| **实验内容** | 1) 它是最简单的一种扫描技术，所利用的是TCP协议的3次握手过程。它直接连到目标端口并完成一个完整的3次握手过程（SYN、SYN/ACK和ACK）。系统提供“connect()”函数完成系统调用，连接目标计算机的端口。如果端口处于侦听状态，那么“connect()”函数就能成功。否则，这个端口是不能用的，即没有提供服务。  2) 客户端与服务器建立TCP连接要进行一次三次握手，如果进行了一次成功的三次握手，则说明端口开放。  1) SYN 扫描，通过本机的一个端口向对方指定的端口，发送一个TCP的SYN连接建立请求数据报，然后开始等待对方的应答。如果应答数据报中设置了SYN位 和ACK位，那么这个端口是开放的；如果应答数据报是一个RST连接复位数据报，则对方的端口是关闭的。  2) 扫描器向目标主机的一个端口发送请求连接的SYN包，扫描器在收到SYN/ACK后，不是发送的ACK应答而是发送RST包请求断开连接。这样，三次握手就没有完成，无法建立正常的TCP连接，因此，这次扫描就不会被记录到系统日志中。这种扫描技术一般不会在目标主机上留下扫描痕迹。  http://10.11.52.15/upload/init/initimage/1489483654805/image002.jpg | | |
| **实验类型**  （打☑） | ☑验证性 □演示性 □设计性 □综合性 | | |
| **实验的重点、难点** |  | | |
| **实验环境** | (1) 互联网环境或者本地主机。  (2) 目标域名自由选做，建议在本地主机部署Web站点，然后扫描本地站点的网络漏洞，增强网络安全意识。 | | |
| **实验的实施阶段** | **实验步骤及实验结果** | **一、扫描开放80端口服务器**  1.1 客户端想要连接服务器80端口时，会先发送一个带有 SYN 标识和端口号的 TCP 数据包给服务器。如果端口是开放的，则服务器会接受这个连接并返回一个带有 SYN 和 ACK 标识的数据包给客户端。随后客户端会返回带有 ACK 和 RST 标识的数据包，此时客户端与服务器建立了连接。如果完成一次三次握手，那么服务器上对应的端口肯定就是开放的。  http://10.11.52.15/upload/init/initimage/1489483654805/image004.jpg  图1  1.2 当客户端发送一个带有 SYN 标识和端口号的 TCP 数据包给服务器后，如果服务器端返回一个带 RST 标识的数据包，则说明端口处于关闭状态。  http://10.11.52.15/upload/init/initimage/1489483654805/image005.jpg  图2  1.3 打开主机B上的“网络协议分析软件”，单击工具栏”过滤器“-〉”添加“-〉”类型过滤器“->”TCP协议“->”接受”->”设置参数”-〉”确定“，然后单击”开始“按钮，捕捉TCP数据包。**实验截图**3**如下**    1.4 打开主机D的终端,输入命令”cd /home/1”、“./open.py”,向主机B发送TCP数据包，显示收到5个数据包。**实验截图**4**如下**    1.5 在主机B上，单击“会话树”中的“192.168.1.3<==>192.168.1.5[4]”,在数据交互图中显示出三次握手的过程。**实验截图**5**如下**    1.6 单击第一个数据包，主机D向主机B发送标志位为SYN数据包。**实验截图**6**如下**    1.7 单击第二个数据包，主机B向主机D发送标志位为SYN|ACK数据包。**实验截图**7**如下**  1.8 单击第三个数据包，主机D向主机B发送标志位为RST数据包，RST包用于强制关闭TCP链接。**实验截图**8**如下**    1.9 单击第四个数据包，主机D向主机B发送标志位为RST|ACK数据包，在释放TCP连接的同时，完成了对前面已接收报文的确认。**实验截图**9**如下**    **二、扫描关闭80端口服务器**  2.1 在主机A上按1.3步骤的方法打开和设置网络协议分析软件。打开主机D的终端,输入命令”cd /home/1”、“./closed.py”,向主机A发送TCP数据包，显示收到2个数据包(主机A打开协议分析软件，软件设置参照主机B)。**实验截图**10**如下**    2.2 在主机A上，单击“会话树”中的“192.168.1.2<==>192.168.1.5[2]”,在数据交互图中显示握手的过程。**实验截图**11**如下**    2.3 单击第一个数据包，主机D向主机A发送一个ACK确认数据包。**实验截图**12**如下**    2.4 单击第二个数据包，由于主机A并没有开放80端口，主机A向主机D发送一个RST|ACK确认数据包, 在释放TCP连接的同时，对前面已接收到的报文进行确认。**实验截图**13**如下**    **一、扫描开放80端口服务器**  1.1 客户端向服务器发送一个带有 SYN 标识和端口号的数据包，如果目标端口开发，则会返回带有 SYN 和 ACK 标识的 TCP 数据包。但是，客户端不会返回 RST+ACK 而是返回一个只带有 RST 标识的数据包。主要用于躲避防火墙的检测。  http://10.11.52.15/upload/init/initimage/1489483655270/image003.jpg  图1  1.2 当客户端发送一个带有 SYN 标识和端口号的 TCP 数据包给服务器后，如果服务器端返回一个带 RST 标识的数据包，则说明端口处于关闭状态。  绘图3(PORT IS CLOSED)  图2  1.3 打开主机B上的“网络协议分析软件”，单击工具栏”过滤器“-〉”添加“-〉”类型过滤器“->”TCP协议“->”接受”->”设置参数”-〉”确定“，然后单击”开始“按钮，捕捉TCP数据包。**实验截图**3**如下**  1.4 打开主机D的终端,输入命令”nmap -sS -p 80 192.168.1.3”,向主机B发送SYN数据包，扫描结果显示主机B的80端口开放。**实验截图**4**如下**    1.5 在主机B上，单击“会话树”中的“192.168.1.3<==>192.168.1.5[3]”,在会话树窗口显示主机D和主机B的数据包交互过程。**实验截图**5**如下**    1.6 单击第一个数据包，主机D向主机B发送标志位为SYN数据包。**实验截图**6**如下**    1.7 单击第二个数据包，主机B向主机D发送标志位为SYN|ACK数据包。**实验截图**7**如下**    1.8 单击第三个数据包，主机D向主机B发送标志位为RST数据包，RST包用于强制关闭TCP链接。**实验截图**8**如下**    **二、扫描关闭80端口服务器**  2.1 在主机A上使用1.3步骤同样的方法打开和设置网络协议分析软件。打开主机D的终端,输入命令”nmap -sS -p 80 192.168.1.2”,向主机A发送SYN数据包，扫描结果显示主机A的80端口关闭。**实验截图**9**如下**    2.2 在主机A上，单击“会话树”中的“192.168.1.2<==>192.168.1.5[2]”,在数据交互图中显示握手的过程。**实验截图**10**如下**    2.3 单击第一个数据包，主机D向主机A发送一个SYN确认数据包。**实验截图**11**如下**    2.4 单击第二个数据包，由于主机A并没有开放80端口，主机A向主机D发送一个RST|ACK确认数据包, 在释放TCP连接的同时，对前面已接收到的报文进行确认。**实验截图**12**如下** | | |
| **实验结果的处理阶段** | **实验结果的分析与总结** | 1．在TCP连接断开时，一共需要发送几个数据包？  4个，顺序如下：   1. 发送一个FIN数据包给对方，表示自己已经没有数据包要发送了，但是依然可以接受对方的数据。 2. 2.收到对方的ACK确认数据包，表示对方已经收到自己的FIN数据包，同意关闭连接 3. 发送一个ACK确认数据包给对方，表示自己已经收到了对方的ACK确认数据包 4. 收到对方的FIN数据包，表示对方也已经没数据要发送了，然后发送一个ACK确认数据包给对方，表示自己已经收到对方的Fin数据包，同意连接关闭。这个ack数据包可以携带一些最后的数据，这个数据包称为最后的ack数据包。 | | |