|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 姓名： | | 学号： | 专业年级：软件工程2020 | 班级： 卓越班 |
| 分组： | | 实验室： | 指导教师：郭念 | 实验日期：2022.04.28 |
| **实验的准备阶段**  **(指导教师填写)** | **课程名称** | **计算机网络与安全** | | |
| **实验名称** | **实验二 IP 与 ICMP 分析** | | |
| **实验目的** | 熟练使用 Wireshark 软件，观察 IP数据报的基本结构，分析数据报的分片；掌握基于 ICMP 协议的 ping 和 traceroute 命令其工作原理ࣿ。 | | |
| **实验内容** | 启动 Wireshark，捕捉网络命令执行过程中本机接受和发送的数据报。  1. 执行 ping 命令，观察 IP 数据报和 ICMP 询问报文的结构：通过 Wireshark 监视 器观察捕获流量中的 ICMP 询问报文和 IP 数据报的结构。注意比较 ICMP 请求 帧与回应帧，ࣿ其 IP 头部数据字段的异同。  2. 改变 ping 命令的参数，观察 IP 数据报分片：更改 ping 命令参数 MTU，使其发 出长报文以触发 IP 数据报分片，再观察 IP 数据报的结构变化。  3. 执行 Traceroute 命令，观察 ICMP 差错报文的结构，并分析其工作原理：使用 Linux 操作系统提供的 traceroute 命令（或者 Windows 系统提供的 tracert 命令）， 捕获和分析该命令所产生的 IP 数据报，特别注意相关的 ICMP 差错报文。结合 捕获的具体数据，画出命令执行过程中数据交互的示意图，掌握 traceroute 的工 作原理。 | | |
| **实验类型**  （打☑） | ☑验证性 □演示性 □设计性 □综合性 | | |
| **实验的重点、难点** | 1. 分析IP数据包结构； 2. 分析ICMP 协议 | | |
| **实验环境** | 1. PC 机一台，连入局域网； 2. Wireshark 软件，建议 3.0 以上版本。 | | |
| **实验的实施阶段** | **实验步骤及实验结果** | **2.1 ping命令**  本机（示例 IP 为 192.168.1.251）启动 Wireshark 软件，选择要监听的网络接口（如 eth0、wlan0）；然后在终端发起网络命令：ping IP 地址/域名。  1. 在 Wireshark 监视器中设置过滤条件，过滤条件为 icmp，则显 出所捕获的 ICMP 数据包。**实验结果截图如下：**    2. 点击 Internet Protocol Version 4 展开，查看 IP 数据报，特别观察 IP 数据报的首部字段ࣿ其内容。 **实验结果截图如下：**    3.点击 Internet Control Message Protocol 展开，查看 ICMP 报文，并解 释回显（Echo Request 和 Echo Reply）报文的首部字段。**实验结果截图如下：**    4. 清空 Wireshark 监控器，重新发起网络命令：  ping IP地址/域名 –l #length，并解释对比前后两次执行 ping 命令的结果。其中，-l #length 确定 echo 数据报的长度为 #length，其默认值为 32 字节，且小于 65,527 字节。 **实验结果截图如下：**    5. 可以多次改变 #length 的大小（例如 1000 字节、2000 字节和 4000 字节），观察 IP 数据报何时会分片？请解释 IP 数据报分片的原因和具体情况。  答：  MTU即允许发送不需要分段的最大IP单包字节数。Data-length=MTU-IP头-iCMP头  使用ping IP地址/域名–l#length，命令，当length+IP头+ICMP头<=MTU时，包不会被分片否则会被分片发送  提示：请先确 认该网络的 MTU，可在 Wireshark 记录中查找“IPv4 fragments”项目。**实验结果截图如下：**    **2.2 traceroute命令**  本机（示例 IP 为 192.168.1.251）启动 Wireshark 软件，选择要监听的网络接口（如eth0、wlan0）；然后在终端发起网络命令：traceroute IP 地址/域名。**实验结果截图如下：**    1. 启动 Wireshark 软件，选择要监听的网络接口，设置过滤条件 icmp。**实验结果截图如下：**    2. 在终端中使用 traceroute 命令，目的主机是外网的一台设备。 **实验结果截图如下：**    3. 点击 Internet Control Message Protocol 展开，查看 ICMP 差错报文，观察并解释 ICMP 报文结构和字段内容。**实验结果截图如下：**    4. 结合 ICMP 报文记录画出数据交互示意图，并描述 tracert 工作原理。  1、tracert发出TTL值为1的ICMP数据包（40个字节、源地址、目标地址和发出时间标签，一般发3个）  2、当到达路径上第一个路由器时，路由器会将，TTL值减1  3、此时TTL值为0，该路由器将此数据包丢弃，向源地址返回一个ICMP超时通知（数据包的源地址、路由器的IP地址）  4、当tracert收到该数据包，获得了这个路径上的第一个路由器的地址  5、tracert再发送另一个TTL为2的数据包  6、第一个路由器会将此数据包转发给第二个路由器  7、当TTL=0，第二个路由器返回一个超时通知，tracert得到第二个路由器地址  Tracert每次发出数据报时便会将TTL加1，发现下一个路由器。这个动作一直重复，直到到达目的地或者确定目标主机不可到达为止，到达目的IP后，目标主机并不返回超时报文。Tracert发送数据报时，会选择一个一般应用程序不会使用的号码来做端口（3000以上），当到达目的地后，目标主机返回一个ICMP port unreachable（端口不可达）的消息。当tracert收到这个消息后，就知道目的地到达了 | | |
| **实验结果的处理阶段** | **实验结果的分析与总结** | 1. 在有线局域网中，PC1 的 IP 地址为 192.168.1.5/24，默认路由器的 IP 地址为 192.168.1.1；PC2的IP地址为192.168.2.6/24，默认路由器的IP地址为192.168.2.1。 在 PC1 向 PC2 发送数据的传输过程中，以太网数据帧的首部字段和 IP 数据报的首部字段是怎样变化的？如果有条件，请搭建实验平台进行实验，并使用 Wireshark 软件验证你的答案。  答：根据通信协议，PC1要传输的数据首先在应用层进行封装，成为数据报文， 数据报文依次经过经过表示层 会话层 传输层进行数据编码，会话协商及传输通道协商后送到网络层进行封装，转变为数据包，打上IP包头，然后经过数据链路层打上帧头封装成数据帧， 最后数据帧送往物理层，以BITS的形式在物理线路上传输到对端PC2. 数据比特流通过物理层传输到对端PC2上 将PC1上的步骤倒过来，层层解封装， 数据比特流解封装为数据帧，数据帧解封装为数据包，最后转化为用户应用程序识别的数据报文。  2. 拒绝服务（Denial of Service，DoS）攻击，DoS 通过消耗目标主机设备的某种资 源，导致其网络服务不能被正常用户使用。  (a) IP 数据报分片机制可能被攻击者利用来构建拒绝服务攻击。试设计一种利 用 IP 数据报分片机制发动 DoS 攻击的方法，并提出防御的思路。  答：  ①设计的攻击的方法：如果一个系统在一分钟之内只能处理10个数据包，攻击者却每分钟向它发送20个数据包，这时，当合法用户要连接系统时，用户将得不到访问权，因为系统资源已经不足。通过控制大量机器实现分布式拒绝服务攻击成为此类攻击方法的主要形式。  ②防御思路：由于进行这种攻击时，攻击者必须连续地向系统发送数据包。当攻击者不向系统发送数据包时，攻击停止，系统也就恢复正常了。此攻击方法攻击者要耗费很多精力，因为他必须不断地发送数据。所以，在大多数情况下，恢复系统需要部分的人为干预，并且有固定人员定期检查系统的安全状况，便可以防御此种类型的攻击。  (b) 请思考利用 ICMP 报文构建 DoS 攻击的可能性以ࣿ防御方法。  答：ICMP 报文构建 DoS 攻击的可行性比较高，ICMP攻击导致拒绝服务(DoS)的方法可以分为三类：  ①针对带宽的DoS攻击：主要是利用无用的数据来耗尽网络带宽。Pingflood、pong、echok、flushot、fraggle 和 bloop是常用的ICMP攻击工具。通过高速发送大量的ICMP [Echo](http://www.yesky.com/key/2749/212749.html" \t "https://codeantenna.com/a/_blank) Reply数据包，目标网络的带宽瞬间就会被耗尽，阻止合法的数据通过网络。  ②针对连接的DoS攻击：可以终止现有的网络连接。针对网络连接的DoS攻击会影响所有的IP设备，因为它使用了合法的ICMP消息。  ③还有一些攻击使用ICMP [Source](http://www.yesky.com/key/3081/168081.html" \t "https://codeantenna.com/a/_blank) Quench消息，导致网络流量变慢，甚至停止。Redirect和Router Announcement消息被利用来强制受害主机使用一个并不存在的路由器，或者把数据包路由到攻击者的机器，进行攻击。  防御方法：针对连接的DoS攻击不能通过打补丁的方式加以解决，通过过滤适当的ICMP消息类型，一般防火墙可以阻止此类攻击。  3. 在实际操作中，Traceroute 命令返回的某些条目以“\*”号表示。请思考有哪些原 因可能导致这样的情况。  答：  1）可能是防火墙封掉了ICMP的返回信息，所以我们得不到什么相关的数据包返回数据。  2）中间任何一个router上如果封了ICMP Echo Request ， traceroute就不能工作 ；中间的router看不到 ，但能看到packet 到达了最后的destination；如果封了ICMP Echo Reply，中间的全能看到，最后的destination看不到。  4. 发送方要怎样决定 IP 数据报分组大小，才能避免因为不同网络 MTU 不一致而 引起分片呢？  答：探测路径最小MTU，发送探测IP包，在包头中设置不可分片，然后通过是否受到ICMP消息即可确定路径MTU。限制最长数据报，一般不要超过1480字节，即以太网MTU（1500）——IP首部（20）。  5. 从 PC1 给 PC2（其地址为 #IP）发送三个 ping 命令，请比较命令的结果，并用 Wireshark 软件进行观察分析。  (a) ping #IP -l 1472 -f -n 1      (b) ping #IP -l 1473 -f -n 1      (c) ping #IP -l 1472 -n 1 | | |