黑马程序员
www.itheima.com
传智播客旗下
高端IT教育品牌

网络攻防的艺术

TCP 协议篇

议题

1. 网络攻防概述
2. TCP 协议工作原理
3. TCP SYN FLood 攻击及其防护技术
4. TCP Reset 攻击
5. 讨论话题： 会用攻击命令（工具）就好，何必了解工作原理

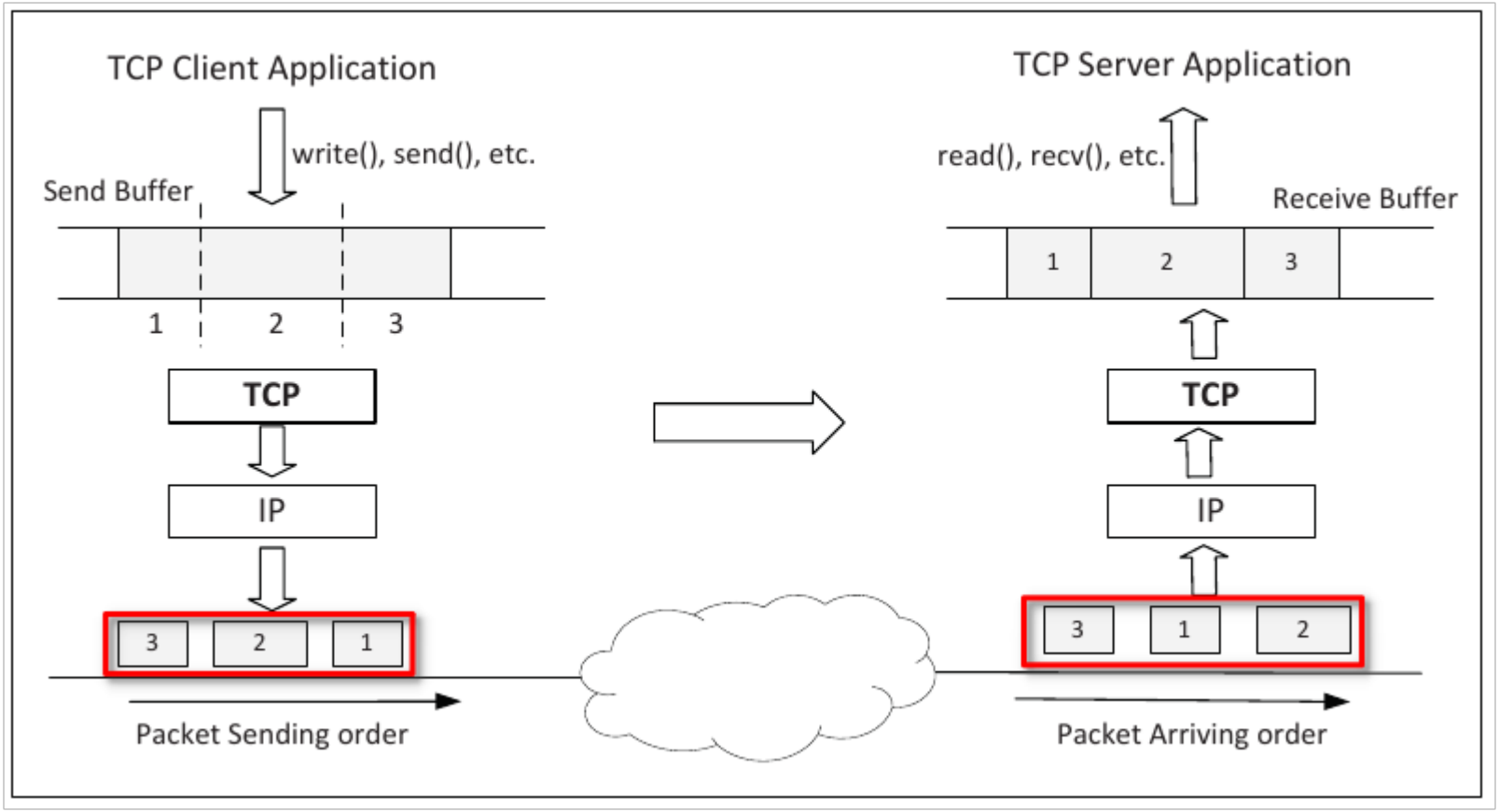
网络攻防概述

1. 网络攻防的三种形式
   - 系统安全攻防
     - 利用软件安全漏洞
   - 网络安全攻防
     - 利用网络协议栈“安全漏洞”
   - 物理攻击 / 社会工程学
     - 利用物理设计缺陷 / 人的心里弱点

TCP 协议的工作原理

1. TCP Client 小程序
2. TCP Server 小程序
3. 掀开数据传输的面纱

掀开数据传输的面纱


TCP Client Application
write(), send(), etc.
Send Buffer
1
2
3
TCP
IP
3
2
1
Packet Sending order
TCP Server Application
read(), recv(), etc.
Receive Buffer
1
2
3
TCP
IP
3
1
2
Packet Arriving order

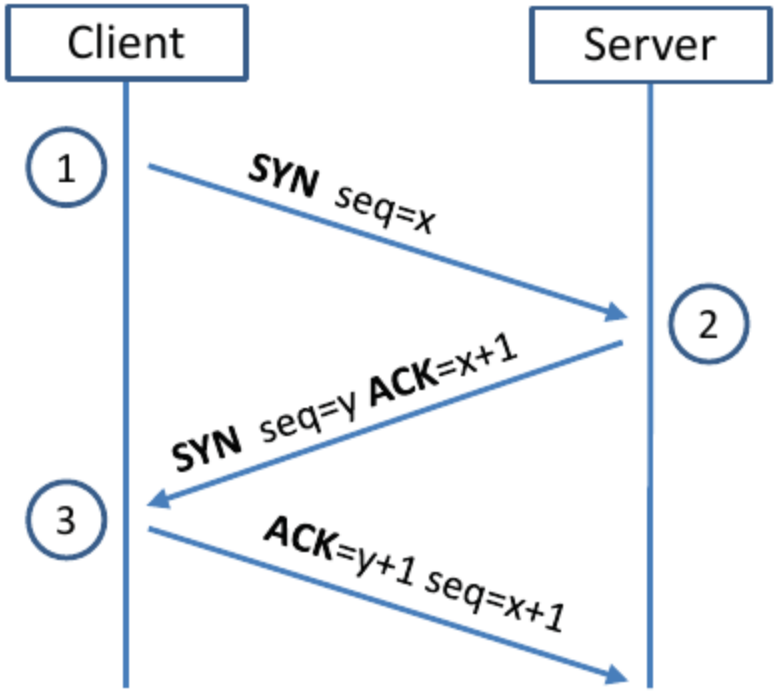
掀开数据传输的面纱

1. 当连接建立完成后，系统分别为 Client 和 Server 准备两个 buffer ， 一个是 SendBuffer ，用于发送数据， 一个是 ReceiveBuffer ，用于接收数据 。
2. 数据的发送： 程序通过接口 write/send/sendto/sendmsg 将要发送的数据写入 SendBuffer ，完成发送。
3. 数据接收： 程序通过接口 read/recv/recvfrom/recvmsg 从 ReceiveBuffer 读入数据，完成数据接收。
4. 详细见上图所示。

TCP SYN Flood 攻击

1. TCP 建立连接过程（三次握手）
2. SYN Flood 攻击
3. TCP SYN Flood 攻击的防护手段

TCP 建立连接的过程



(a) TCP 3-way Handshake

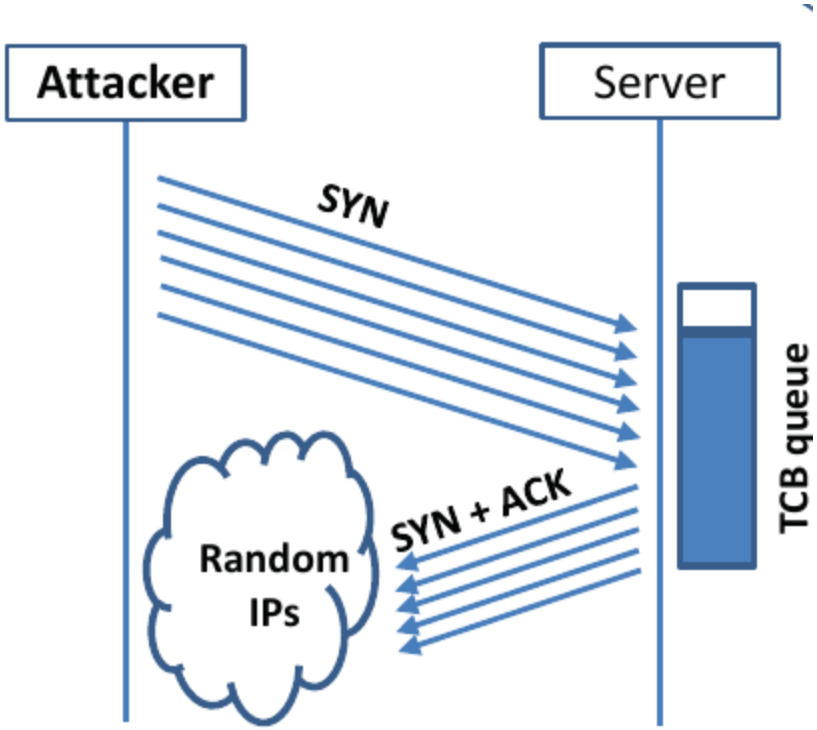
TCP 建立连接的过程

1. TCP 提供面向连接的服务， 因此数据发送前需要先通过三次握手建立连接：
   - 第一次握手： 首先客户端 C （？）主动发起连接，发送 SYN （连接请求标志）， 以及序号 SEQ=x （序号 x 随机生成）到服务器端 S 。
   - 第二次握手： 服务器端 S 接受到 SYN 后， 向客户端 C 也发送 SYN 及 ACK ， 且 ack=x+1，以及序号 Seq=y （序号 y 随机生成）。
   - 第三次握手： 客户端接到 SYN 及 ACK 后， 核查 ack 是否为 x+1，若正确， 则客户端 C 发送 ACK 且 ack=y+1 ，至服务器端 S 。
   - 服务器端 S 接收到 ACK ，核查 ack 是否为 y+1. 若正确，则连接正常建立。

TCP SYN Flood 攻击

1. TCP SYN Flood 攻击策略思考：
   - 从连接建立流程可知， Client 端发起 SYN 标志， Server 端需要应答 SYN+ACK ，并等待 Client 的应答 ACK ，完成连接建立流程。
   - 假设此时（还未接到 Client 的 ACK 应答）又有新的 SYN 连接请求到达，就需要在 Server 端维持一个半连接队列，用于管理还未完成三次握手的连接请求。
   - 如果发起 SYN 请求的 Client 过多，那么在 Server 端就需要维持一个较大的队列来管理这些半连接请求。
   - 如果 Server 端没有收到 Client 端来的 ACK 应答（如 ACK 包丢失）包，那么 Server 端需要超时重发 SYN+ACK 包， 并继续等待
   - 总上，模拟 Client 端发送大量的 SYN 请求，阻塞 Server 端对新的连接请求响应，就是我们的攻击策略

TCP SYN Flood 攻击



(b) SYN Flooding Attack

TCP SYN Flood 攻击的防护手段

1. 从攻击的手法也可以很好的制定防护的策略，一般是减少 SYN+ACK 重传的次数，增大半连接的队列长度，启用 SYNcookies ，因此 linux 内核提供如下三个参数达成上述要求
2. 半连接队列的长度， 默认 128
   - tcp_max_syn_backlog
3. SYN+ACK 重传次数，默认 5
   - tcp_synack_retries
4. 启用 SYN cookies 机制， 默认启用
   - tcp_syncookies

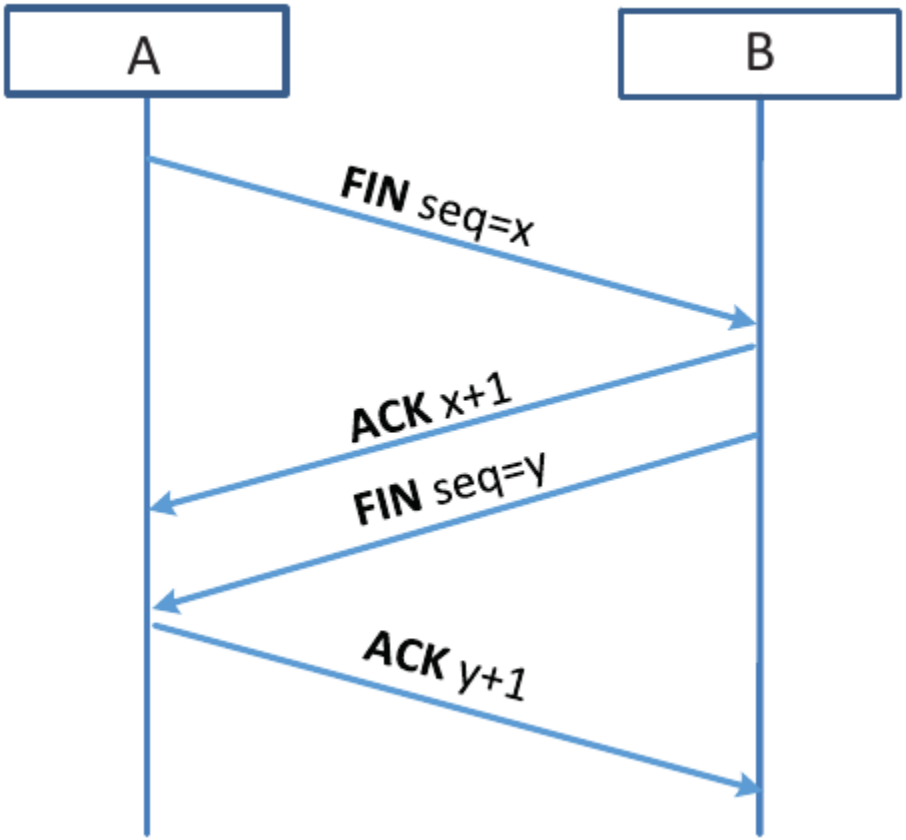
TCP Reset 攻击

1. TCP 正常断开连接（四次挥手）
2. TCP 异常断开连接（ RST or SYN ）
3. Reset 攻击实施

TCP 正常断开连接（四次挥手）

1. 连接断开，并不是必须由 Client 发起， Server 端同样也可以主动断开连接，下文以 A 、 B 指带 Client 和 Server 两端。
2. 第一次挥手， A 端发出 FIN 断开连接请求
3. 第二次挥手， B 端收到 FIN 请求后，答复 ACK
4. 当 A 端接收到 ACK 后，处于半连接状态，注意，此时可以接收数据，但不可以发送数据。
5. 第三次挥手：当 B 端的 Buffer 数据发送完毕后， 发出 FIN 断开连接请求。
6. 第四次挥手：当 A 端收到 B 端的 FIN 请求后，处理完成接收 Buffer 里的数据后， 应答 ACK 。
7. B 端接收到 ACK 应答，至此， TCP 连接正常断开。
8. 相信见下图

TCP 断开连接（四次挥手）



TCP 异常断开连接

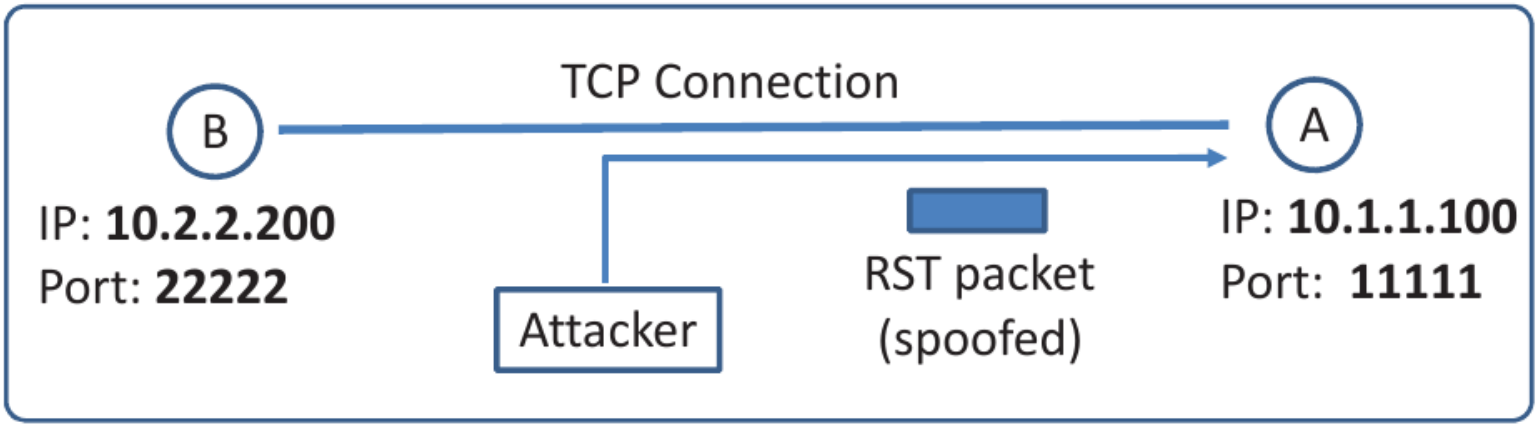
1.TCP 连接的异常断开可以分为两种情况：

- TCP 连接的一端（以 A 端指代，可以是 Client ，也可以是 Server ）收到 RST 复位包， A 端强制断开连接并丢弃缓冲区数据。
- TCP 连接的一端（以 A 端指代，可以是 Client ，也可以是 Server ）收到 SYN 连接请求包， A 端强制端口断开链接，丢弃缓冲区数据，并发送 RST 包给 B 端。

TCP Reset 攻击实施

1. 针对 TCP 连接两端中的一端，以第三者的身份，伪造一个对端发送过来的数据包，且包含 SYN 或者 RST 。是为我们实施 TCP Reset 攻击的策略。

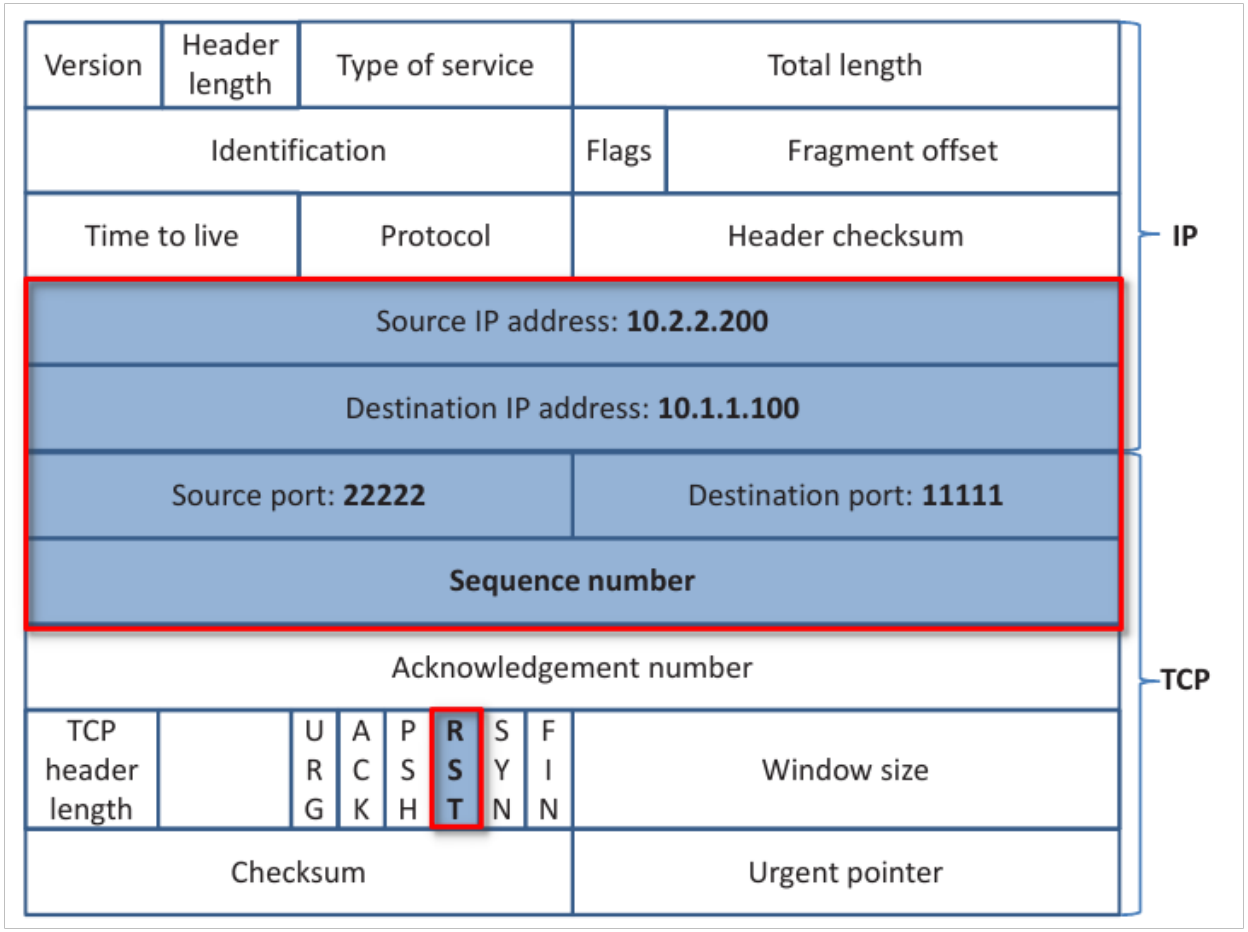
   - TCP Reset 攻击的实施情况，见下图所述。



TCP Reset 攻击 -- 伪造数据包

1. 伪造攻击数据，最重要的是要获取被攻击连接如下信息：
   - 源地址
   - 目的地址
   - 源端口号
   - 目的端口号
   - 数据包序号

TCP Reset 攻击 - 伪造攻击包



TCP Reset 攻击防护

1. 限制 MAC 地址 （？）
2. 限制网络信息包的获取 （？）
3. 大数据分析 （？）
4. 设置防火墙， 丢弃带 RST 包

讨论：

1. 会用攻击命令（工具）就好，何必了解工作原理

安全行业的现状

1. 求贤若渴，缺人，缺能出“成绩”的高手。
2. 不差钱
   - 以最近 facebook 泄漏用户信息事件为例，如果能通过漏洞挖掘、渗透测试等安全验证手段，解决 facebook 的信息泄漏问题，我想让扎克伯格兄台拿出万分之一的罚款（2 亿美金），养一个能解决问题的安全团队，他是会非常乐意的。
   - 一般来讲，要求安全的企业（电商、银行、证卷等），一旦不安全了（信息泄漏、 DDOS 攻击）等，信誉受到影响，对企业来讲是致命的。

Facebook灭顶之灾！或遭200000000000美元罚款！

2018-03-23 07:45:20

来源：深蓝财经 2人参与 1评论

Facebook 陷入史上最大规模数据泄漏丑闻，有超过 5000 万用户的信息数据被泄漏。

Thank You!

改变中国 IT 教育，我们正在行动

www.itcast.cn