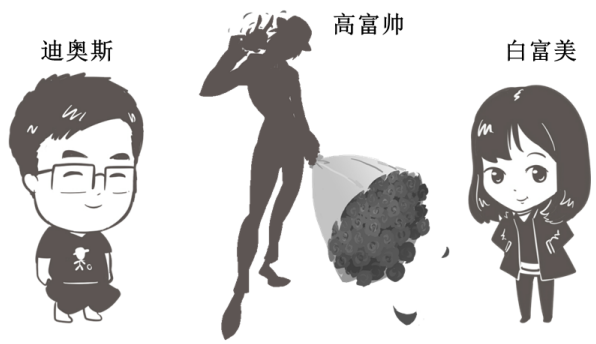
网络是建立在各种协议之上的。TCP/IP在其制订之初，没有考虑安全因素,导致他本身无安全可言。
由于它自身的缺陷，导致这种攻击很难防御，而这种攻击对于如今的信息安全又有着重大的影响。

所以我们给大家科普一些看似深奥，然而其实是比较有意思的黑客攻击方法。

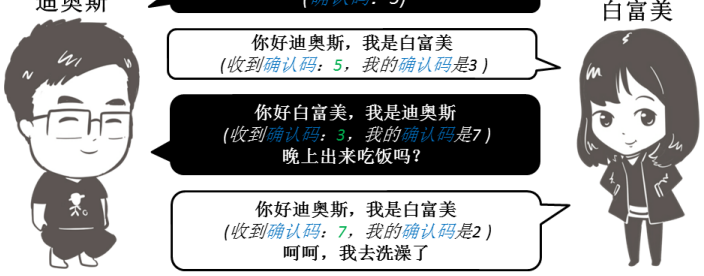
这种专业的东西你觉得你能听的懂么？

说的好像你能听懂一样～～

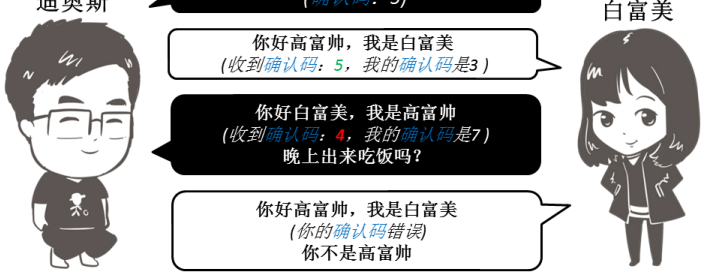
在讲TCP欺骗攻击之前，我们先描述一下TCP协议最基本的三次握手，这是TCP协议的根本。我们请出三个人物来协助演示。
(这三个人物名字所对应的,是计算机的IP地址)

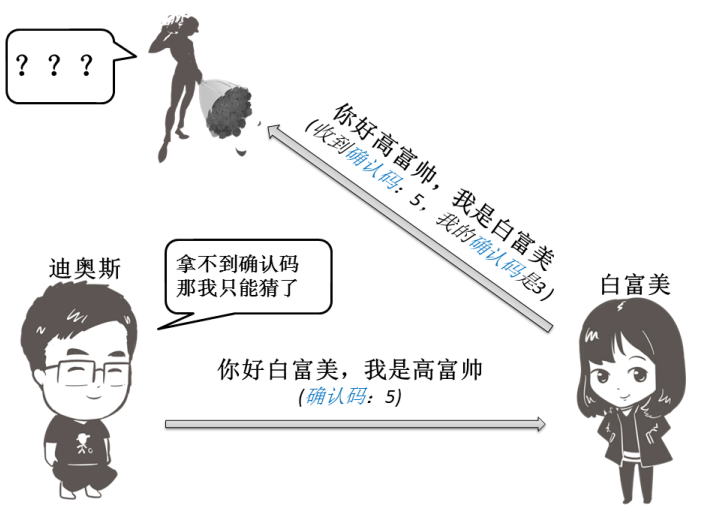


TCP三次握手通常是这样的，确认码是随机的，它的作用是确认数据包是否被对方所接收，以保证可靠传输。



迪奥斯被白富美女神这样敷衍，非常不爽，他想知道白富美是怎么跟高富帅聊天的，所以他就冒充高富帅...但是有一个问题，他拿不到白富美给高富帅的确认码。

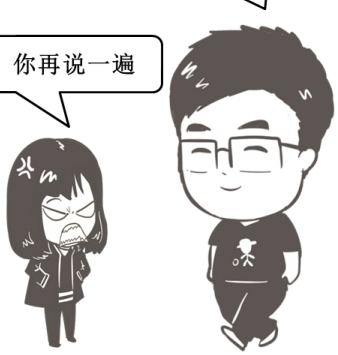




上面这就是迪奥斯拿不到确认码的原因，他的高富帅身份只是在传输的数据包中伪装的，白富美收到消息后会去找真正的高富帅确认。然而迪奥斯并没有放弃，攻击还在继续...

这个白富美好傻哦～

你再说一遍



TCP协议在这个时候就是那么傻。
对于确认码不正确的猜测攻击的数据包会被直接丢弃并被要求关闭连接，但是这中间还是留下一段足够利用的时间。

后记：
在上面这个例子中，白富美从始至终不知道迪奥斯的存在，并且不知道这个高富帅是伪造的。他的攻击目的在于劫持会话，窃取关键信息。
这就有一个前提，那就是高富帅不会发类似于“这到底怎么回事？”的数据包。不过这不是太大的问题因为这个伪造的高富帅并不需要真实存在。

另外值得一提的是，确认码的猜测并不是那么容易的。猜测的数字可以从2的32次方(40多亿)一直递减到0，这就是另一种攻击思路。用数目巨大的确认码数据包来欺骗服务器，骗取服务器对每个数据包做出应答，从而消耗它的资源直至瘫痪，这种攻击叫做SYN泛洪攻击，是以破坏为目的的攻击。