**网络安全技术第二次作业**

2017221302009

陆圣珩

**测试点2-1**

1. **在查询相关技术资料或进行实际验证的基础上回答以下问题：**

* **如果主机A跳过与主机B建立TCP连接的前两个步骤，直接发送三次握手中最后一个带ACK标志的包，主机B会如何处理？**

主机B 会将其判断为错误包，不做处理

* **如果应用程序在释放连接的过程中（参见教材图2-6-3），由于应用程序异常终止来不及通知TCP协议释放连接，试问在实际情况中应该如何处理这种异常。**

1）当TCP连接的进程在忘记关闭Socket而退出、程序崩溃、或非正常方式结束进程的情况下：（Windows客户端），会导致TCP连接的对端进程产生“104: Connection reset by peer”（Linux下）或“10054: An existing connection was forcibly closed by the remote host”（Windows下）错误。

2）当TCP连接的进程机器发生死机、系统突然重启、网线松动或网络不通等情况下：Windows客户端），连接的对端进程可能检测不到任何异常，并最后等待“超时”才断开TCP连接。

1. **IP协议安全威胁产生的根本原因是什么？请举例分析。**

IP协议本身没有验证源IP地址真实性的机制。比如拒绝服务攻击可以以此避免追踪以及基于IP地址认证的网络服务欺骗便是针对这一缺陷进行攻击的。

1. **TCP协议安全威胁产生的根本原因是什么？请举例分析。**

TCP三次握手过程需要存储连接状态，因此会产生系统开销。

拒绝服务攻击，可以针对TCP三次握手，不发送ACK包，以极小开销进行攻击。

1. **UDP协议安全威胁产生的根本原因是什么？请举例分析。**

UDP 协议本身无连接、不可靠、不保序的特点。

比如UDP假冒与UDP劫持本质上是因为UDP协议的特点加上IP协议欺骗完成的。

1. **域名解析协议中主要存在哪些安全威胁？简要说明威胁过程和原理。**

流量型拒绝服务攻击，如UDP flood、TCP flood、DNS请求flood，和PING flood等。

异常请求访问攻击，如超长域名请求、异常域名请求等，这类型攻击的特点是通过发掘DNS服务器的漏洞 ，通过伪造特定的请求报文，导致DNS服务器软件工作异常而退出或崩溃而无法启动，达到影响DNS服务器正常工作的目的

DNS劫持攻击，如篡改LDNS缓存内容、篡改授权域内容、ARP欺骗劫持授权域、分光劫持等，这种类型攻击的特点是通过直接篡改解析记录或在解析记录传递过程中篡改其内容或抢先应答，从而达到影响解析结果的目的