第二讲 网络协议安全性分析

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：

1） 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 将丢弃该包不做任何处理

2）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。

通信另一方有一个时钟，当时钟时间耗尽并且其间没有收到会话时断开连接

2、 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 地址真实性的机制以及有最大传输单元限制

例如基于 IP 地址认证的网络服务欺骗从而假冒可信的 IP 地址而非法访问计算机资源和 IP 碎片攻击

3、 TCP 协议安全威胁产生的根本原因是什么？请举例分析。

TCP 使用三次握手机制来建立一条连接，需要耗费一定资源和时间。其间可能的威胁有：

1. 攻击者监听 B 方发出的 SYN/ACK 报文。

2. 攻击者向方发送 RST 包，接着发送 SYN 包，假冒 A 方发起新的连接。

3. B 方响应新连接，并发送连接响应报文 SYN/ACK。

4. 攻击者再假冒 A 方对 B 方发送 ACK 包

为此可以产生很多攻击，例如 SYN Flooding 和 ACK Flooding 等

4、 UDP 协议安全威胁产生的根本原因是什么？请举例分析。

UDP 并不面向连接，提供的是不可靠的服务

以此有 UDP 假冒和 UDP 劫持

5、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。

DNS 查询和应答是基于 UDP 的应用。有 DNS 欺骗、生日攻击、DNS 缓存毒化和基于 DNS 的 DDos

DNS 欺骗原理：如果可以冒充域名服务器，然后把查询的 IP 地址设为攻击者的 IP 地址，这样的话，用户上网就只能看到攻击者的主页，而不是用户想要取得的网站的主页了，这就是 DNS 欺骗的基本原理。

DNS 缓存毒化