第二次作业

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：**

一、 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？

答：主机 B 收到该包以后应该会会直接丢弃。因为没有前两次握手，没为主机 A 的连接创造资源。

二、 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。

答：应用程序异常终止则会停止 TCP 报文的发送，在交互的双方中的某一方长期未收到来自对方的确认报文，则其在超出一定的重传次数或时间后，会主动向对端发送 reset 报文释放该 TCP 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。**

答：根本原因是 IP 协议设计时自身的缺陷，

a) IP 协议本身没有验证源 IP 地址真实性的机制，导致攻击者可以进行 IP 假冒攻击；
b) 链路层具有最大传输单元 MTU 这个特性，它限制了数据帧的最大长度，不同的网络类型都有一个上限值，以太网的 MTU 是 1500。如果 IP 层有数据包要传，而且数据包的长度超过了 MTU，那么 IP 层就要对数据包进行分片(fragmentation)操作，使每一片的长度都小于或等于 MTU。IP 首部有两个字节表示整个 IP 数据包的长度，所以 IP 数据包最长只能为 0xFFFF，就是 65535 字节。如果有意发送总长度超过 65535 的 IP 碎片，或构造畸形的 IP 碎片，部分老的操作系统在进行碎片重组处理时会导致崩溃或拒绝服务。

3、 **TCP 协议安全威胁产生的根本原因是什么？请举例分析。**

答：根本原因是 TCP 协议设计时自身的缺陷和实际实现的缺陷

a) 三次握手过程需要存储连接状态，因此会产生系统开销，攻击者可以短时间内向受害者发送大量 TCP 请求耗尽受害者的资源，形成拒绝服务攻击。
b) 攻击者向服务器发送众多的带有虚假地址的请求，服务器发送回复信息后等待回传信息，由于地址是伪造的，服务器接收不到回传的消息，但不会立即释放资源，攻击者反复传送伪地址请求，服务器资源最终会被耗尽。

4、 **UDP 协议安全威胁产生的根本原因是什么？请举例分析。**

答：根本原因是 UDP 设计时自身的缺陷。

1） UDP 是无连接的，因此攻击者可以假冒被攻击者的 IP 地址向服务器发送请求，服务器则会把数据返回给被攻击者，而如果攻击者可以窃听 UDP 应答包，则可以假冒被攻击者的身份来获取所需的信息，形成 UDP 假冒攻击。

2） 被攻击者发出 UDP 请求后，攻击者假冒服务器发送 UDP 应答，虽然服务器的应答也可以到达客户端，但如果客户端的操作已经触发，就有可能造成损失。

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。

一、 DNS 欺骗：

客户端以特定的标识 ID 向 DNS 服务器发送域名查询数据包
DNS 服务器查询之后以同样的 ID 返回给客户端响应数据包
攻击者拦截该响应数据包，并修改其内容，返回给客户端

二、 DNS 猜测攻击

攻击者向域名服务器发送对某一主机域名的大量查询，然后发送大量猜测 ID 的伪造应答数据包，从而使得域名服务器上的对该主机域名的 IP 保存的是攻击者提供的假 IP，当其他用户访问时，就会被引向错误的网站无法而正常访问。

三、 DNS 缓存毒化

攻击者拥有自己的一个域和一个已经被攻陷的 DNS 服务器。攻击者通过查询自己所控制的域的域名，使本地服务器和被攻陷的 DNS 服务器进行通信，并且使被控制的服务器回复对攻击者所拥有的域的查询，然后通过区域传送的方式将错误的或者被篡改过的 DNS 信息返回给本地域名服务器。当其他用户向本地域名服务器查询某一被篡改过的域名时，服务器会返回攻击者篡改过的 IP 地址。