1.IP欺骗攻击及防御技术

A.安全原由:IP协议不能保证数据就是从数据包中给定的源地址发出的，你绝对不能靠对源地址的有效性检验来判断数据包的真假；

B.IP欺骗攻击：攻击者发送含有伪造返回地址的数据包。

2.基本的IP欺骗(基本原理、防范)

最基本的IP欺骗技术有三种：

a.简单的IP地址变化

b.源路由攻击

c.利用Unix系统的信任关系

3.DNS欺骗及防御技术—DNS工作原理

DNS的全称是域名服务器，当一台主机发送一个请求要求解析某个域名时，它会首先把解析请求发到自己的DNS服务器上。

4.DNS欺骗及防御技术—DNS欺骗的原理及实现步骤

原理：而入侵者欲实现DNS欺骗，关键的一个条件就是在DNS服务器的本地Cache中缓存一条伪造的解析记录。

两种可能情况：

A.攻击者可以控制本地的域名服务器

B.攻击者无法控制任何DNS服务器（关键在于获取目标DNS服务器的ID号)

1. DNS欺骗及防御技术—DNS欺骗的局限性及防御

A.局限性：

a.攻击者不能替换缓存中已经存在的记录,但可以增加记录

b.DNS服务器存在缓存刷新时间问题

B.防御(六点)：

a.使用最新版本DNS服务器软件并及时安装补丁。

b.关闭DNS服务器的递归功能。

c.限制区域传输范围。

d.限制动态更新；

e.采用分层的DNS体系结构。

1. Web欺骗及防御技术—Web欺骗的概念（网络钓鱼）

Web欺骗是一种电子信息欺骗，攻击者创造了一个完整的令人信服的Web世界，但实际上它却是一个虚假的复制。Web欺骗能够成功的关键是在受害者和真实Web服务器之间插入攻击者的Web服务器，这种攻击常被称为“中间人攻击”。

1. Web欺骗及防御技术—Web欺骗的防御

A.配置网络浏览器使它总能显示目的URL，并且习惯查看它。

B.检查源代码，如果发生了URL重定向，就一定会发现。

C.使用反网络钓鱼软件。

D.禁用JavaScript、ActiveX或者任何其他在本地执行的脚本语言。

E.确保应用有效和能适当地跟踪用户。无论是使用cookie还是会话ID，都应该确保要尽可F.能的长和随机。

G.培养用户注意浏览器地址线上显示的URL的好习惯。培养用户的安全意识和对开发人员的安全教育。