# 网络安全简介

# 1.1.1 网络安全为什么重要

网络应用已渗透到现代社会生活的各个方面；电子商务、电子政务、电子银行等无不关注网络安全。网络安全上到国家安全，下至每个人的生活。信息安全空间将成为传统的国界、领海、领空的三大国防和基于太空的第四国防之外的第五国防，称为cyber-space。

# 1.1.2 信息安全的概念

| 层 | 协议名称 | 攻击类型 | 原因 |
| --- | --- | --- | --- |
| 网络层 | ARP | ARP欺骗 | ARP缓存的更新机制 |
| | IP | IP欺骗 | IP层数据包是不需要认证 |
| | ICMP | ICMP Flood攻击 | 利用Ping |
| 传输层 | TCP | SYN Flood攻击 | TCP三次握手机制 |
| | UDP | UDP Flood攻击 | UDP非面向连接的机制 |
| 应用层 | FTP、SMTP | 监听 | 明文传输 |
| | DNS | DNS Flood攻击 | DNS的递归查询 |
| | HTTP | 慢速连接攻击 | HTTP的会话保持 |

# 信息安全基础概念

## 信息安全的重要性

信息安全指的是保护信息免受未授权访问、使用、披露、破坏、修改或破坏的过程，确保信息的机密性、完整性和可用性。

## 信息安全的重要性

在数字化时代，信息安全对于保护个人隐私、企业资产和国家安全至关重要。信息泄露可能导致经济损失、信誉损害甚至政治动荡。

## 信息安全的三大支柱

信息安全的三大支柱包括技术、管理和法律。技术措施如加密和防火墙，管理措施如风险评估和安全政策，法律措施则涉及合规性和法律框架。

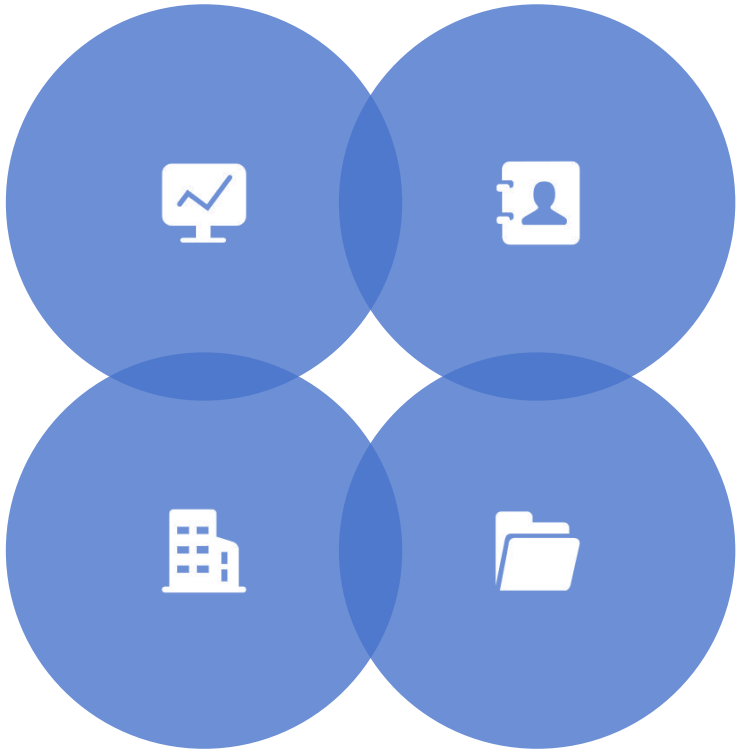
# 网络系统脆弱性的原因分析

## 开放性网络环境的影响

开放性的网络环境使得网络系统暴露在各种潜在的威胁之下，增加了遭受攻击的风险。由于互联网的全球性和连通性，恶意用户可以轻易地发现并利用网络系统中的漏洞。

## 操作系统存在的安全缺陷

操作系统作为网络系统的基础平台，其安全缺陷直接影响整个系统的稳定性。由于操作系统的复杂性，它们往往包含许多未被发现的安全漏洞，攻击者可以利用这些漏洞获得系统控制权。



## 协议设计的固有脆弱性

网络协议在设计时往往更注重功能性和互操作性，而安全性考虑不足，导致协议本身存在固有的脆弱性。例如，早期的TCP/IP协议栈缺乏足够的加密和身份验证机制，容易被攻击者利用。

## 应用软件漏洞的普遍性

应用软件是用户与网络系统交互的直接界面，其漏洞的普遍性是导致网络系统脆弱的重要原因。软件开发者可能在编码过程中引入安全漏洞，如缓冲区溢出、SQL注入等，这些漏洞可被攻击者利用来执行恶意代码。

# 网络安全的基本要素

## 保密性

保密性确保信息不被未授权的个人、实体或进程访问，保护数据免遭泄露。

## 完整性

完整性保证信息在存储、传输或处理过程中不被未授权的修改或破坏。


## 可用性

可用性确保授权用户在需要时能够及时访问和使用信息。

## 可控性

可控性涉及对信息和信息系统访问的控制，确保只有授权用户才能进行操作。

## 不可否认性

不可否认性确保信息的发送者和接收者不能否认其操作，为交易和通信提供法律证据。