

攻击者利用网络系统存在的漏洞和安全缺陷对网络系统的硬件、软件及其系统中 的数据进行的攻击 主动攻击 被动攻击 硬件、软件、协议的具体实现或系统安全策略上存在缺陷 PING扫描 信息的收集 OS探测、穿透防火墙探测、端口扫描 漏洞扫描 系统安全漏洞扫描 实施攻击 巩固攻击成果 网络嗅探技术 只限于局域网 共享式局域网 使用集线器或共用一条总线的局域网 交换式局域网 检测和防范 使目标主机停止提供服务 耗尽目标主机的通信、存储或计算资源的方式 拒绝服务攻击DoS 将多台主机联合起来作为攻击平台,对一个或多个目标发动DoS攻击,从而成倍 分布式拒绝服务攻击DDoS 地提高拒绝服务攻击的威力 主机设置 防火墙 网络设备设置 路由器 覆盖了缓冲区周围的内存空间。黑客借此精心构造填充数据,导致原有流程的改 变,让程序转而执行特殊的代码,最终获取控制权。 利用某些数据库的外部接口把用户数据插入到实际的数据库操作语言当中,从而 达到入侵数据库乃至操作系统的目的。 寻找SQL注入点、获取和验证SQL注入点、获取信息、实施直接控制和间接进行控 主控模块 感染模块 计算机病毒和恶意软件 触发模块 破坏模块