

06

网络安全技术

防火墙

- ◆ 防火墙是在内部网络和外部因特网之间增加的一道安全防护措施，分为网络级防火墙和应用级防火墙。
- ◆ 网络级防火墙层次低，但是效率高，因为其使用包过滤和状态监测手段，一般只检验网络包外在(起始地址、状态)属性是否异常，若异常，则过滤掉，不与内网通信，因此对应用和用户是透明的。
- ◆ 但是这样的问题是，如果遇到伪装的危险数据包就没办法过滤，此时，就要依靠应用级防火墙，层次高，效率低，因为应用级防火墙会将网络包拆开，具体检查里面的数据是否有问题，会消耗大量时间，造成效率低下，但是安全强度高。



入侵检测系统IDS

- ◆ 防火墙技术主要是分隔来自外网的威胁，却对来自内网的直接攻击无能为力，此时就要用到入侵检测IDS技术，位于防火墙之后的第二道屏障，作为防火墙技术的补充。
- ◆ 原理：监控当前系统/用户行为，使用入侵检测分析引擎进行分析，这里包含一个知识库系统，囊括了历史行为、特定行为模式等操作，将当前行为和知识库进行匹配，就能检测出当前行为是否是入侵行为，如果是入侵，则记录证据并上报给系统和防火墙，交由它们处理。
- ◆ 不同于防火墙，IDS入侵检测系统是一个监听设备，没有跨接在任何链路上，无须网络流量流经它便可以工作。因此，对IDS的部署，唯一的要求是：IDS应当挂接在所有所关注流量都必须流经的链路上。因此，IDS在交换式网络中的位置一般选择在：
 - ① 尽可能靠近攻击源；
 - ② 尽可能靠近受保护资源。

网络安全技术

◆ 入侵防御系统IPS

IDS和防火墙技术都是在入侵行为已经发生后所做的检测和分析，而IPS是能够提前发现入侵行为，在其还没有进入安全网络之前就防御。

在安全网络之前的链路上挂载入侵防御系统IPS，可以实时检测入侵行为，并直接进行阻断，这是与IDS的区别，要注意。

◆ 杀毒软件

用于检测和解决计算机病毒，与防火墙和IDS要区分，计算机病毒要靠杀毒软件，防火墙是处理网络上的非法攻击。

◆ 蜜罐系统

伪造一个蜜罐网络引诱黑客攻击，蜜罐网络被攻击不影响安全网络，并且可以借此了解黑客攻击的手段和原理，从而对安全系统进行升级和优化。



网络安全技术

◆ 网络攻击和威胁

攻击类型	攻击名称	描述
被动攻击	窃听（网络监听）	用各种可能的合法或非法的手段窃取系统中的信息资源和敏感信息。
	业务流分析	通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从而发现有价值的信息和规律。
	非法登录	有些资料将这种方式归为被动攻击方式。

主动攻击	假冒身份	通过欺骗通信系统（或用户）达到非法用户冒充成为合法用户，或者特权小的用户冒充成为特权大的用户的用户的目的。黑客大多是采用假冒进行攻击。
	抵赖	这是一种来自用户的攻击，比如：否认自己曾经发布过的某条消息、伪造一份对方来信等。
	旁路控制	攻击者利用系统的安全缺陷或安全性上的脆弱之处获得非授权的权利或特权。
	重放攻击	所截获的某次合法的通信数据拷贝，出于非法的目的而被重新发送。
	拒绝服务（DOS）	对信息或其它资源的合法访问被无条件地阻止。