IDS的自防护原则与技术途径 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/251/2021_2022_IDS_E7_9A_84_E8_87_AA_E9_c101_251031.htm 自身安全是网络 安全系统的一个重要特性，如果没有完善的自身防护体系作为保障，即使拥有再强大的功能也无法实现。如同其他信息安全产品一样，IDS自防护问题一直都是IDS研发与实际应用中的一个热点问题。 目前IDS自防护体系的建立仅仅把IDS作为一般的信息系统考虑，而在实际的网络安全防御系统中，IDS是一类工作在敌对网络环境下具有指挥控制特点的防御系统。IDS自防护除了考虑作为一般信息防御系统的自防护外，还必须考虑在攻防对抗环境下的IDS的生存问题。 IDS的体系结构 IDS是一类在网络攻防对抗环境中实现网络入侵检测、预警、评估与响应的指挥控制系统，其体系结构如图1所示。 图1 IDS的体系结构 IDS从网络或主机获取信息，然后依据现有知识对获取信息进行检测、识别、评估并依据检测结果做出相应告警与响应。信息的获取、判断、响应是一个循环过程，这与对抗中广泛应用的OODA环（观察、适应、决策、行动）相一致。 IDS的六类脆弱点 在攻防对抗条件下，根据IDS的体系结构，IDS可表现出如图2所示的六类脆弱点。 这六类脆弱点分别是传感器与链路脆弱点、攻击检测脆弱点、状态和威胁评估脆弱点、融合系统知识库脆弱点、传感器/信号源控制系统脆弱点以及传感器行为检测脆弱点。 1、传感器与链路脆弱点。攻击者影响传感器和信息链路，抑制正确的信息并插入错误的信息； 2、攻击检测脆弱点。攻击者通过对传感器（如干扰或欺骗）或对攻击检测的直接渗透，降低系统集

成、关联、跟踪效能及对单个目标的检测识别能力；3、状态和威胁评估脆弱点。攻击者通过组合具有特殊结构的数据或信息，降低或欺骗入侵行为的推断程序性能；4、融合系统知识库脆弱点。攻击者一旦获得对融合的数据库或操作显示部分的访问，将会暴露传感器和融合系统中可用于信息攻击的一些性能；5、传感器/信号源控制系统脆弱点。对传感器控制的攻击会使传感器丧失工作能力或降低工作性能；6、传感器行为监测脆弱点。攻击者对传感器行为进行监测（尤其是主动传感器），以观察融合系统的行为，推断它的关注焦点及信息需求，以及收集计划的周期和方式。 IDS面临的四类威胁 在攻防对抗条件下，对于不同类型和不同程度的攻击，攻击者想取得的效果并不相同，即攻击者对IDS的OODA环的预期影响程度、方式不同。按照攻击的效果，总体上可以将IDS面临的威胁分为四类。 1、利用：攻击者根据公开获取的可用于攻击系统的信息、融合系统获取的信息、监测攻击是否成功的信息实现对IDS系统的工作机制、工作过程的分析。 2、欺骗：“ 欺骗 ”的目的是要导致融合系统用户做出错误的决策。对融合系统采用“ 欺骗 ”时，各种刺激因素要与融合处理知识协调一致。只有这样，才会产生错误数据和错误融合决策。 3、干扰：对传感器融合系统的干扰将会对融合处理所用信息的可用性或准确性产生影响。干扰方法包括传感器的干扰、网络上的“ 洪水 ”广播、过载以及对所选链路或融合节点实施的软件或暂时性干扰。 4、破坏：软硬件破坏基于物理手段实施，这一实施过程需要建立在基于对融合节点进行准确定位的基础上。 IDS的自防护原则与技术途径 建立IDS的自防护体系必须从体系、算法和软

件三个层面综合考虑，在建立IDS自防护体系的过程中，应遵循以下原则：多渠道防护原则，应保证防护手段的多样性，采用多种技术实现对脆弱点的冗余保护；协调使用原则，应对IDS采用的防护策略和技术进行统一配置，协调管理；信息保密原则，随着IDS的发展，IDS内部通信量不断增加，应坚持不明文传输的原则，才能有效地保证不被攻击者窃听到IDS内部行为；综合防护原则，应从多方面对IDS进行有效的防护，技术与管理并重，以确保IDS自防护系统的生存能力。
对IDS信息源的防护是实施IDS自防护的重要内容之一。IDS传感器获取信息的位置分为本地、远程和混合三种。从获取信息的冗余程度来划分，信息源分为冗余信息源、补充信息源和所需全部信息源。一般而言，IDS信息源主要有三种分布方式：冗余和紧密、效能、分布式和非独立。 表1列出了三种信息源分布结构的技术特征及可能遭受的攻击方式。针对不同的攻击方式，结合各信息源结构的技术特征，可采取不同的技术手段构筑信息源的自防护体系。 总而言之，IDS是一类在网络空间具有指挥控制特点的信息防御系统，围绕IDS的信息攻击与防御是网络攻防的焦点之一。可以说，任何一项IDS技术，若不能抵御针对IDS的信息攻击，那么将导致全面失效。IDS自防护体系的建立除了考虑作为一般信息系统的自防护外，还必须考虑在网络攻防对抗环境下的自防护问题。 