IPS/IDS

一，IPS(Intrusion Prevention System)

IPS全称是(Intrusion Prevention System)，中文翻译为“入侵检测系统“，能够识别入侵事件，关联、冲击、方向和适当的分析，之后将合适的信息发送到防火墙，交换机和其他网络设备之中，可减轻相应的安全风险。

IPS是对防病毒软件(Antivirus Programe)和防火墙(Packet Filter ,Application Gateway)的补充，IPS可以隔离和中断及调整一些具有危险性的网络传输行为。

在ISO/OSI网络逻辑模型中，防火墙主要起到了第二层到第四层的作用，而第四曾到第七层是非常薄弱的，而病毒等相关恶意程序则在第五层到第七层起到了严重的威胁，此时为了弥补ISO/OSI逻辑模型的空失。

IPS(Intrusion Prevention System)也就是”入侵检测系统“投入了使用，IPS可以发现网络异常从而发送至防火墙进行处理和应急响应，从而衍生除了”入侵响应系统“(IRS:Intrusion Response System)主要针对入侵系统进行响应那个，与IPS连着配合，从而使得入侵预防系统进一步发展。

IPS是对防火墙的一种补充，而不是一种替代，IPS可以防御防火墙所不能防护的一些深层威胁，可以对网络、数据等方面进行保护，相对来更像是一种风险控制的安全产品。

而IDS是一种入侵检测系统，想对于IPS来说，IDS是主动的，IPS是被动的，IDS可以根据异常的，可能存在入侵行为的进行检测和响应，并告知相关的解决方案，总结来说IDS更像是一个类似与风险管理的安全产品。

二，IDS(Intrusion Detection System)

IDS的全称为(Intrusion Detection System)，中文为”入侵检测系统“，主要通过定制安全策略，对软件、硬件、网络、系统等运行状态进行监视。以保证系统的完整性和可能性，而IDS的作用就相当于一个监控设备，实时检测每一个空间的运行状况，如果出现安全问题则发出警告。

IDS(Intrusion Detection System)主要起源于1980年James P.Anderson所著的《计算机安全威胁监控与监视》（《Computer Security Threat Monitoring and Surveillance》）在此书中，首次详细阐述了入侵检测概念，并提出了计算机系统威胁分类及利用审计跟踪数据监视入侵活动的思想，此后被业内公认为入侵检测的开山之作。

入侵检测主要分为事实检测和事后检测两种检测手法，实施检测在网络连接过程中进行，系统根据用户历史行为模型，并结合计算机中的专家知识以及神经网络模型对用户当前的操作进行判断。

而后入侵检测则是由相关安全专业人士进行，是一个不定期进行的检测，后入侵检测的综合能力并不如实时入侵检测能力更有效。

CIDF

CIDF全称为（Common Intrusion Detection Framework）中文是”通用入侵检测框架“CIDF意图在某种程度将如请作为标准化，并开发一些应用程序接口。

CIDF主要阐述了一个入侵检测系统的通用模型，主要分为如下组件：

事件生产器（Event generators）

事件分析器（Event analyzers）

响应单元（Response units）

事件数据库（Event databases）

CIDF将IDS需要分析的数据统称为”事件(event)“，他可以是一个网络数据包，也可能是系统日志等途径信息。

分类

按照入侵检测手段，IDS如请检测模型分为基于网络和基于主机两种方法

1,基于主机模型

基于主机模型也称为基于系统的模型，他是通过分析系统的审计数据来发现有可以的数据流，比如内存和文件变化等，其输入的数据主要来源与系统的审计日志，一般只能检查该主机发生入侵。

该模型的有点主要分为如下几点：

性能价格：在主机数量少的情况下，这种方法的性能价格比可能更高;

更加细致：可以更容易检测到一些活动，比如敏感的文件目录、程序以及端口存取，而这些活动很难在基于协议的线索中进行发现。

视野集中：一旦入侵者得到了一个主机名和用户名口令，基于主机的代理最有可能区分于正常活和非法活动。

易于剪裁：每一个主机都有自己的代理，用户剪裁更加方便。

较少主机：基于主机的方法又是不需要增加专门的硬件平台

流量不敏：用代理的方式一般不会因为网络流量的增加而丢掉对网络行为的监视

2,基于网络模型

通过链接在网络上的站带你捕捉网络上的包，并分析其是否具有已知的攻击模式，以此来判别是否为入侵者。当该模型发现某些可疑现象时也会一样产生警告，并且会向一个中心管理站点发出”告警“信号。

主要分别为如下几个特点：

侦测速度：基于网络的检测器通常在微秒或秒级发现，而大多数基于主机的产品则要依赖对最近几分钟内审计记录并进行分析

隐蔽性：一个网络上的侦测器并不像一个主机一样那么容易被存取，因此也不容易遭受到攻击。由于不是主机，因此一个网络的监视器不用去相应ping，不允许别人存取本地存储器，不能让别人运行，而且不让多个用户使用他

视野更广：基于网络的方法可以用作网络边缘撒谎那个，及攻击者还没能接入网络时则会被禁止

较少监视器：由于一个监视器就可以保护一个共享网段，所以你不需要很多检测器，相反的，如果甚至于主机，则在每个主机都需要一个代理，这样的话，话费更高。难于管理，但是，如果在一个交换环境喜爱，诶个主机就要配一个检测器，因为每个主机都在自己的网段上。

占用资源：在被保护的设备上不用占用任何资源

互补性：基于网络可以能够客观的反映网络活动，特别能够监视到主机审计系统的盲区，而基于主机的模型能股更加准确的监视主机中的各种活动，基于网络模型受到交换网的限制，只能监控同一监控点的主机，而基于主机模型装有IDS监控主机可以对同一监控点的所有主机进行监控

按照入侵检测的技术基础可以分为两类，一种标志的入侵检测（Signature-based），另一种是基于异常情况的入侵检测（Anomaly-based）.

对于基于标识技术来说，首先要定义违背安全策略的事件特征，如网络数据包某些头部信息，检测主要判断是否有相同的特征，这也和一些杀毒软原理类似。

而异常的检测技术则是通过先定义一组系统”正常“情况的数值，比如CPU利用率，内存利用率，文件校验和等。然后将数值与所定义的”正常“情况比较，得出是否有被攻击的迹象，这种检测方式的核心在于如何确定议所谓的”正常“情况。

3.输入如请检测系统：

基于主机入侵检测系统：其输入数据来源于审计日志，一般只能检测主机上发生的入侵。

基于网络的入侵检测系统：其输入的数据来源于网络的信息流，能够检测该网段上发生的网络入侵。

采用上述两种数据的分布式入侵检测系统，他能够同时分析来源数据的审计日志和来源于网络的信息流，这种系统一般由多个部件组成

按照入侵检测所采用的技术方法又可以将其细分为下面四种方法：

一是基于用户行为概率统计模型的入侵方法：

这种入侵方法是对用户历史行为建模，或在早期的证据模型的基础上，实时检测用户对系用的使用情况，根据系用内部保存的用户行为概括统计模型进行检测，当发现，有可以用户行为时，立即保持跟踪并监视记录该用户行为，系统要根据每个月那个胡以前的历史行为，生成每个用户的行为记录，当用户改变他们的行为习惯时，这种一场也会被检测起来。

4.基于神经网络的入侵检测方法

这种方法是利用神经网络进行检测，主要依据哟过户行为具有学习和自适应能力，能够根据实际检测到的信息有效加以处理并作出是否有入侵行为的判断，但是该想法并没有成熟比较完善的产品。

5.基于专家的入侵检测技术

该技术主要根据安全专家对可以行为而制定的一些规则，然后再次基础撒谎那个建立相应的专家系统，由此专家系用自动对所涉及的入侵行为进行分析，该系统可以随着经验的累计不断的自我进行学习，并进行规则的扩充和修正，

6.基于模型推理的入侵技术

该技术根据入侵这在进行入侵时所执行一些行为程序特征，建立u一种入侵行为模型，并依据这种行为模型代表的去入侵行为特征来判断用户是否存在入侵行为。当然这种方法也是建立在当前已知的如请行为程序的基础之上，对未知的入侵方法所执行的一些行为程序模型识别需要进行学习和扩展。

以上几种方法每一种都不能保证准确的检测出变化多端的入侵行为，因此在网络安全防护中需要充分衡量个各种方法的弊端，综合运用这些方法才能够包杂货那个有效的检测出入侵者的非法行为。

流程

1,信息搜集

信息搜集包含系统、网络，数据及用户行为活动状态和行为，信息搜集需要在计算机网络系统中找到不同的关键点来进行，这样一方面可以尽最大可能的扩大范围，另一方面从信息来源的信息不一致性是可以性能各位或存在入侵的最好标识，因为有时候一个信号源收到的信息可能看不出来可疑点。

2,系用日志

黑客经常在系统日志中留下他的踪迹，因此，充分的利用系统日志是检测入侵的必要条件，日志文件那种记录了各种行为类型，每种行为类型又包含了各种不同的信息，很显然的对于用户来讲，不正常或期望的行为，就是重复登入失败，登入到不到期望的位置以及不期望的位置以及非授权的企业访问重要文件等。

3,目录以及文件中的异常改变

网络环境中的文件系用包含很多数据文件，包含重要的信息的文件和私有数据我二年经常是黑客修改或破坏的目标

4,物理形式的入侵信息

这包括两个方面的内容，一是为授权对网络硬件的连接，二是对物理资源的未授权访问。

5,数据分析

一般通过三种技术手段进行分析，模式匹配，统计分析和完整性分析，其中前两种方法用于实时入侵检测，而完整性分析则用于事后分析

6,匹配模式

_模式匹配就是将搜集到的信息与已知的网络入侵和系用误用模式数据库进行比较，从而发现违背安全策略的行为，该方法的一大有点是只需要搜集相关的数据集合，显著减少系统负担，且技术已经相当成熟，他与病毒防火墙采用的方法一样，检测准确率和效率相当的高，但是，该方法存在的弱点是需要不断的升级以及对付不断出现的黑客攻击手法，不能检测从前从未出现过的黑客攻击手段，

7,统计分析

系统分析方法首先给系统对象，（如用户，文件，目录设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数，操作失败次数延时等）。测量属性的平均值将被用于来网络，系用的行为进行比较，任何观察值，如果超过了正常范围，默认就会有入侵事情发生。

其优点是可以检测到未知的如请和更为复杂的入侵，而缺点是误报，漏报率非常高，且不使用一年过户正常行为的突然改变，具体的统计分析如基于专家系统的，基于模型的推理的和基于神经网络的分析方法，这在前面入侵检测分类中已经提到，喜爱面对统计分析的模型做以介绍，

入侵检测5种统计模型

操作模型

该模型假设异常可通过测量结果与一些固定指标相比较得到，固定指标可以根据经验或一段时间内判断统计平均得到，举例来说，在段时间内多次失败登入很有可能尝试口令攻击

方差

计算参数方差并设定其置信区间，当测量超过置信区间范围时表明有可能是异常

多元模型

即操作模型的扩产，它通过同时分析u的讴歌参数实现检测

马尔柯夫过程模型

即将每种类型的事件定义为系统状态，用状态转移矩阵来表示状态的变化，当一个事件发生时，如果在矩阵中该转移的概率较小则该可能是异常时间

时间序列分析

即将时间计数与资源耗用根据时间排成序列，如果一个新时间在该时间发生的概率极低，则该时间可能是入侵

统计方法的最大优点是它可以”学习“用户的使用习惯，从而具有较高检出率与可用性，但是它”学习“能力有时也会给入侵者一机会，因为入侵者可以通过逐步”训练“使入侵该事件符合正常操作的统计规律，从而通过入侵检测系统

完整性分析

完整性分析主要关注某个温暖见或对象是否被更改，这经常包括文件和目录的内容属性，他在发现按被修改成类似特洛伊木马的应用程序方面特别有效，其有点是不管模式匹配方法和统计分析能否发现入侵，只要是有入侵行为导致了文件或其他对象的热和改变，他都够发现，缺点是一般一批处理方式实现，不用与实时响应。