 大家好！ 今天通过了CCSP CSIDS 3.0考试。谈一谈学习考试经验，希望对大家有用。 CSIDS 3.0 60题，825分通过，如果选英语为第二语言，时间105分钟。 考试内容可参考考试大纲：
http://www.cisco.com/warp/public/10...ms/9E0-100.html [考试内容] 如果把考试大纲的线条划粗些，可以说，考试主要着重在以下几个方面： 1.攻击与安全的基本知识。 2.IDS Sensor和Module的安装与配置。 3.IDS管理，监控与报告。 4.Sensor和签名的管理 5.IDS维护和内部结构。 与其他考试一样，CSIDS3.0的考试内容与2.x版相差很大，一定要注意书和学习资料与考试大纲相符。考试大纲那两页纸，应该打印出来钉在床头才对。呵呵。 [学习材料] 1.旧版书 (覆盖律 40%) 我买了本CSIDS by Earl Carter，觉得还是很值得的。书很系统地讲解了攻击与防范初步介绍，Cisco安全，IDS概念和网络上的配置等等。在基础知识这部分，书写的很好，没有一点过时的东西(很策略性的)，并且，把IDS原理讲的很清楚。所以，这书还是值得收藏的。现在国内人邮出了中文版，我不知道翻译的效果怎么样，80块人民币也不是什么大数目，大家如果想考IDS，还是应该看这本书的。(当然，有新教材的另说。有新教材的朋友，就不必看我写的东西了，直接去考试就行了。呵呵) 那么书里不必看的是CSPM和Director部分。相应换成了IDS Device Manager和Event Viewer，以及Management/Monitoring Center。下面有介绍。另外，书里

很大一部分是各种Signature的介绍，理解意思就可以，不用钻的太深，如果你想考试而不是先当黑客的话。 2.Cisco Document CD或网页 覆盖率：70% 上面说了，大纲里的IDS Device Management，Event Viewer，Cisco Works MC都是旧版书里没有的，要看网页才行。 IDS Network Sensor 3.1 http://www.cisco.com/univercd/cc/td...s8/13872_01.htm http://www.cisco.com/univercd/cc/td...s8/13870_01.htm IDS Device Management: http://www.cisco.com/univercd/cc/td...s8/13876_01.htm Event Viewer: http://www.cisco.com/univercd/cc/td...s8/13877_01.htm Signature Engine http://www.cisco.com/univercd/cc/td...s8/13869_01.htm (以上都是在IDS 3.1目录下的，大家可以都看一看) http://www.cisco.com/univercd/cc/td...sids8/index.htm 那么Cat 6000上的IDS Module，书上有介绍，但版本不够，网页上有最新的： 3.0 http://www.cisco.com/univercd/cc/td...dsm_2/index.htm IDS内部体系结构，很重要 http://www.cisco.com/univercd/cc/td...ids/0866_02.htm Cisco Works Management Center，介绍性地考了考，参考它的Datasheet, Q&amp.A，和简单的介绍 http://www.cisco.com/en/US/products...literature.html 列的这些资料基本覆盖全了。内容就不算多了。考试考的很细，所以单看书是不行的，要把操作做熟，很熟，要对命令行，文件体系结构，两个GUI界面的所有菜单的所有选项都很熟。要做到这点，就要对着文档做实验。 [实验] 我反复强调实验的

重要性，因为不仅考试有实验操作，而且大量的客观题是考你操作界面的属性，不做实验，实在是背不下来的。那么对於多数朋友，我想都缺乏IDS的操作经验，也缺少实验条件。最好的办法就是有CCO帐号，到Csico e-Learning上做实验。e-Learning实验分3个部分： 1.VoD 有一个教学片，介绍了IDS 3.1，Device Manager，Event Viewer的安装和基本操作。一共一个小时不到，有条件一定要看，能省很多学习时间。强烈推荐。 连接在E-LearningSpecializationVideo on Demand VPN Security下， CTU-NPI-IDS 3.1 Appliance 2.PEC提供的IDS实验。 这是“ 真 ”的实验，不是Flash，连接到IDS 3.1的Console上，并有一台虚拟PC，可以做所有IDS 3。1的实验。包括命令行，目录和体系结构了解，IDS Device Manager， 下载并安装Event Viewer。那么这三个界面占了考试的大部分内容。所以，有条件就要做上10遍8遍。强烈推荐。 3.KnowledgeNet，是Flash型的，一是不自由，二是旧版的，都是CSPM相关的实验，不推荐。 [其他] TK还是要看的。呵呵。 [收获] IDS考下来还是很爽的。 1.这门是黎明前的黑暗。考完后，就看到曙光了。 2.在技术上，没有IDS，就谈不上安全。但由於工作限制，IDS是我们最缺乏经验的。靠考试的方法补足，在技术上翻越了一座小山。说小山是因为只是在基本概念，操作和维护上有了解，对攻击深层理解还差的很远，对Cisco以外的产品理解还没有。但这是迈出的第一步，是很关键的一步。 3.在心理上，过了一关。 