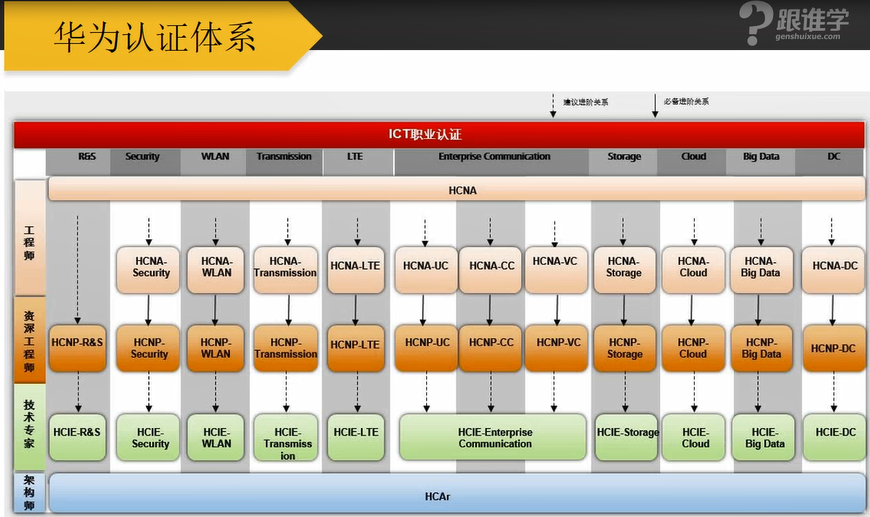
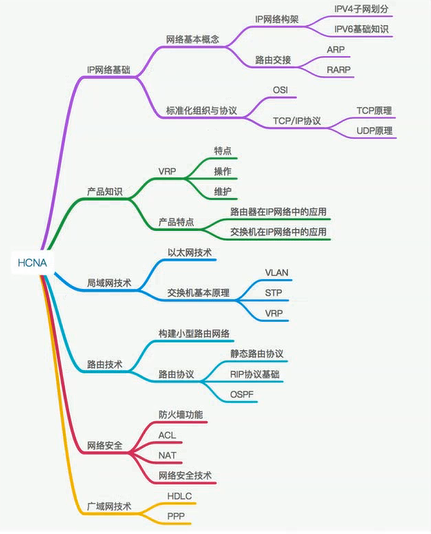
**1.1**



**总目录**



**1.2**

**1.企业网1，校园网2，政务网2（物理隔离），金融网4级网络**

**2..出口，核心，接入**

**1.3**

**1.默认路由是指向外网的数据**

**2.OSPF是出口路由器回程路由**

**3.NAT是转换源地址访问公网**

**一.基础书籍**

计算机网络

计算机网络基础

计算机基础

**二.论坛社区**

1.我不知道是不是《0day安全》这本书，这本书是看雪论坛合作出版的，（看雪的几本书都很赞，比如《加密与解密》、《c++反汇编与逆向分析技术揭秘》），逆向推荐去看看"看雪论坛"。

2.搞Web安全我推荐去乌云，以及乌云知识库

3.图灵社区

**三.计算机三级**

计算机三级视频

链接：[https://pan.baidu.com/s/18JSTk9XdtBc53KpKb7MmRw](http://link.zhihu.com/?target=https%3A//pan.baidu.com/s/18JSTk9XdtBc53KpKb7MmRw) 密码：8yIL

**四，网络安全**

[该怎样学习网络安全？](https://www.zhihu.com/question/23067604/answer/56463462)

[席琴女](https://www.zhihu.com/people/xi-qin-nu)

捍卫自己的梦想

首先，必须（时刻）意识到你是在学习一门可以说是最难的课程，是网络专业领域的顶尖课程，不是什么人、随随便便就能学好的。不然，大家都是黑客，也就没有黑客和网络安全的概念了。

很多朋友抱着学一门课程、读好一本书就可以掌握网络安全的知识和技能。不幸的是，网络安全技术决不是几本书、几个月就可以速成的。你需要参考大量的参考书。

另一方面，在学校接受的传统教育观念使我们习惯由老师来指定教材、参考书。遗憾的是走向了社会，走到工作岗位，没有人给你指定解决这个安全问题需要什么参考书，你得自己研究，自己解决问题。

网络安全涉及的知识面广、术语多、理论知识多。正给学习这门课程带来很多困难。也需要我们投入比其它课程多的时间和精力来学习它。

概括来说，网络安全课程的主要内容包括：

l 安全基本知识

l 应用加密学

l 协议层安全

l Windows安全（攻击与防御）

l Unix/Linux安全（攻击与防御）

l 防火墙技术

l 入侵监测系统

l 审计和日志分析

下面分别对每部分知识介绍相应的具体内容和一些参考书（正像前面提到的那样，有时间、有条件的话，这些书都应该看至少一遍）。

一、安全基本知识

这部分的学习过程相对容易些，可以花相对较少的时间来完成。这部分的内容包括：安全的概念和定义、常见的安全标准等。

大部分关于网络安全基础的书籍都会有这部分内容的介绍。

下面推荐一些和这部分有关的参考书：

l 《CIW：安全专家全息教程》 魏巍 等译，电子工业出版社

l 《计算机系统安全》 曹天杰，高等教育出版社

l 《计算机网络安全导论》 龚俭，东南大学出版社

二、应用加密学

加密学是现代计算机（网络）安全的基础，没有加密技术，任何网络安全都是一纸空谈。

加密技术的应用决不简单地停留在对数据的加密、解密上。密码学除了可以实现数据保密性外、它还可以完成数据完整性校验、用户身份认证、数字签名等功能。

以加密学为基础的PKI（公钥基础设施）是信息安全基础设施的一个重要组成部分，是一种普遍适用的网络安全基础设施。授权管理基础设施、可信时间戳服务系统、安全保密管理系统、统一的安全电子政务平台等的构筑都离不开它的支持。

可以说，加密学的应用贯穿了整个网络安全的学习过程中。因为之前大多数人没有接触过在这方面的内容，这是个弱项、软肋，所以需要花费比其它部分更多的时间和精力来学习。也需要参考更多的参考书。

下面推荐一些和这部分有关的参考书：

l 《密码学》 宋震，万水出版社

l 《密码工程实践指南》 冯登国 等译，清华大学出版社

l 《秘密学导引》 吴世忠 等译，机械工业（这本书内容较深，不必完全阅读，可作为参考）

三、协议层安全

系统学习TCP/IP方面的知识有很多原因。要适当地实施防火墙过滤，安全管理员必须对于TCP/IP的IP层和TCP/UDP层有很深的理解、黑客经常使用TCP/IP堆栈中一部分区或来破坏网络安全等。所以你也必须清楚地了解这些内容。

协议层安全主要涉及和TCP/IP分层模型有关的内容，包括常见协议的工作原理和特点、缺陷、保护或替代措施等等。

下面推荐一些和这部分有关的参考书（经典书籍、不可不看）：

l 《TCP/IP详解 卷1：协议》 范建华 等译，机械工业出版社

l 《用TCP/IP进行网际互联 第一卷原理、协议与结构》 林瑶 等译，电子工业出版社

四、Windows安全（攻击与防御）

因为微软的Windows NT操作系统已被广泛应用，所以它们更容易成为被攻击的目标。

对于Windows安全的学习，其实就是对Windows系统攻击与防御技术的学习。而Windows系统安全的学习内容将包括：用户和组、文件系统、策略、系统默认值、审计以及操作系统本身的漏洞的研究。

这部分的参考书较多，实际上任何一本和Windows攻防有关系的书均可。下面推荐一些和这部分有关的参考书：

l 《黑客攻防实战入门》 邓吉，电子工业出版社

l 《黑客大曝光》 杨继张 等译，清华大学出版社

l 《狙击黑客》 宋震 等译，电子工业出版社

五、Unix/Linux安全（攻击与防御）

随着Linux的市占率越来越高，Linux系统、服务器也被部署得越来越广泛。Unix/Linux系统的安全问题也越来越凸现出来。作为一个网络安全工作者，Linux安全绝对占有网络安全一半的重要性。但是相对Windows系统，普通用户接触到Linux系统的机会不多。Unix/Linux系统本身的学习也是他们必须饿补的一课！

下面是推荐的一套Linux系统管理的参考书。

l 《Red Hat Linux 9桌面应用》 梁如军，机械工业出版社（和网络安全关系不大，可作为参考）

l 《Red Hat Linux 9系统管理》 金洁珩，机械工业出版社

l 《Red Hat Linux 9网络服务》 梁如军，机械工业出版社

除了Unix/Linux系统管理相关的参考书外，这里还给出两本和安全相关的书籍。

l 《Red Hat Linux安全与优化》 邓少鹍，万水出版社

l 《Unix 黑客大曝光》 王一川 译，清华大学出版社

六、防火墙技术

防火墙技术是网络安全中的重要元素，是外网与内网进行通信时的一道屏障，一个哨岗。除了应该深刻理解防火墙技术的种类、工作原理之外，作为一个网络安全的管理人员还应该熟悉各种常见的防火墙的配置、维护。

至少应该了解以下防火墙的简单配置。

l 常见的各种个人防火墙软件的使用

l 基于ACL的包过滤防火墙配置（如基于Windows的IPSec配置、基于Cisco路由器的ACL配置等）

l 基于Linux操作系统的防火墙配置（Ipchains/Iptables）

l ISA配置

l Cisco PIX配置

l Check Point防火墙配置

l 基于Windows、Unix、Cisco路由器的VPN配置

下面推荐一些和这部分有关的参考书：

l 《

网络安全与防火墙技术

》 楚狂，人民邮电出版社

l 《Linux防火墙》

余青霓

译，人民邮电出版社

l 《高级防火墙ISA Server 2000》 李静安，中国铁道出版社

l 《Cisco访问表配置指南》 前导工作室 译，机械工业出版社

l 《Check Point NG安全管理》

王东霞

译，机械工业出版社

l 《虚拟专用网（VPN）精解》 王达，清华大学出版社

七、入侵监测系统（IDS）

防火墙不能对所有应用层的数据包进行分析，会成为网络数据通讯的瓶颈。既便是代理型防火墙也不能检查所有应用层的数据包。

入侵检测是防火墙的合理补充，它通过收集、分析计算机系统、计算机网络介质上的各种有用信息帮助系统管理员发现攻击并进行响应。可以说入侵检测是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。