登录

CISSP考试一次通过指南（文末附福利）

tinyfisher / 2017-12-25 09:27:00 / 浏览数 12408 安全技术 技术讨论 顶(0) 踩(0)

2017年12月19日，在上海黄浦区汉口路亚洲大厦17层通过了CISSP认证考试，拖拉了一年，终于成绩还算令人满意，为攒人品将自己一年多的复习心得和大家分享，希望能

先简单介绍下本人专业背景吧，本科和硕士专业都是信息安全，算得上科班出生，只是学校里的课程没学扎实，基础一般，毕业后在某大型金融机构做安全，渗透、漏扫、S

CISSP介绍

CISSP 英文全称：" Certified Information Systems Security
Professional"，中文全称："(ISC)²注册信息系统安全专家"，由(ISC)²组织和管理，是目前全球范围内最权威，最专业，最系统的信息安全认证。

CISSP的含金量和认可度还是很高的，考试费用也不菲，599刀，涉及的内容非常广泛，号称安全界的"百科全书"，不过虽然涉及的范围广，但很多都是点到为止，
"一英里宽，一英寸深"，这是CISSP最大的特点。

为什么考CISSP？用我们领导的话说，可以迅速建立起个人对安全体系的知识框架，认证+读行业标准是最有效的方法。

CISSP复习攻略

决定了考CISSP之后就要尽快的解决战斗，拖的时间越长越对生活有影响，最好在半年内完成复习和考试，本人这次因为种种原因，拖了一年，深刻感受到战线过长的痛苦。
我的复习材料：All in One的第六版中文版+OSG官方学习指南中文版+官方习题英文版

All in one前前后后看了3遍，OSG看了2遍，这两本教材内容基本差不太多，all in
one讲的比较细，比较啰嗦，OSG和考纲结合得比较紧，内容也比较紧凑，建议大家直接看OSG即可，但务必要多读几遍，对书中的知识点都要弄懂。
CISSP现在最新的考纲包括8个CBK：
• 安全与风险管理 (安全、风险、合规、法律、法规、业务连续性)
• 资产安全 (保护资产的安全性)
• 安全工程 (安全工程与管理)
• 通信与网络安全 (设计和保护网络安全)
• 身份与访问管理 (访问控制和身份管理)
• 安全评估与测试 (设计、执行和分析安全测试)
• 安全运营 (基本概念、调查、事件管理、灾难恢复)
• 软件开发安全 (理解、应用、和实施软件安全)
之所以称之为安全界的"百科全书"，是因为上述8个领域基本涵盖了安全工作中的所有方面，个人在安全评估与测试、安全运营这两个领域有一些实际的经验，其他的领域接
书看完之后可能没有什么感觉，一定要做题，仅仅做书中每个章节的习题是不够的，all in
one的习题比较难，OSG的习题比较简单，建议大家还是做官方的习题集，毕竟是官方出的习题，应该是和考试最接近的材料了，不过现在只有英文版的，对于英语一般的朋

考试技巧

CISSP考试最大的特点是没题库可以背。考试里面直接考概念和定义的题目很少。大量场景题，比如给你一段文字描述，说某企业面临了XX问题，问你最佳解决思路是什么。

考试时间6个小时，大家一定要做好充分的准备，巧克力、红牛、干粮、水都得带足，中间状态不太好的时候可以出来补充能量。时间一般肯定够，所以大家不用特别着急，

多用排除法，有些题目可以迅速排除2个选项，剩下的两个自己拿捏一下，往往正确率还可以。考试现在有中文的，翻译一般没啥问题，但是有的可能还是得看一下英文，往

考试环境一般都是可以的，这次考试和我同一时间的好多都是考GMAT的学生，考试中心给我单独安排了一个单间，还送了耳塞，考试环境很安静，很nice。

最后，不要怕，不过是一个考试而已。套用到实际工作中去，很多题不知道怎么选，我就想象放到我们公司我会怎么做。祝大家都能够通过CISSP考试，我的一些复习材料（
a74r分享给大家，给我的这次备考画上句号。

点击收藏 | 2 关注 | 2
上一篇：Pentest Wiki Part... 下一篇：Pentest Wiki Part...
1. 14 条回复


AAAAAAAAAA 2017-12-25 10:33:00

感谢楼主分享，赞一个

0 回复Ta


shuchao****@sina 2017-12-25 10:33:13

求百度云盘访问的提取码，谢谢！

0 回复Ta


早上起来做运动 2017-12-25 11:21:32

感谢lz分享

0 回复Ta


tinyfisher 2017-12-25 11:41:40

@shuchao**@sina
a74r

0 回复Ta


站着洗澡 2017-12-25 11:42:26

cissp还是要真的花心思去学的，确实增加视野，正如cissp说的，一英寸深一英里长，面广但不深入。
14年的时候参加某安培训，还是有题库的，那时候有真题大概1000题这样。我考完试，背了80多题出来，加上25题不算分，基本学习一下的同学都能过，哈哈我来装个X

0 回复Ta


lin**** 2017-12-25 13:31:47

赞一个，预约的明年考试，希望也能过

0 回复Ta


hades 2017-12-25 15:10:29

@tinyfisher 辛苦了

0 回复Ta


hades 2017-12-25 15:11:41

@站着洗澡 你要放题出来给大伙看看么？？<{= . . . . (嘎~嘎~嘎~)

0 回复Ta


站着洗澡 2017-12-26 09:59:24

@hades 上传不了附件

0 回复Ta


hades 2017-12-26 10:22:07

@站着洗澡 重新开话题帖子吧 回复里面是不能插附件的 (□•□□•□)□□

0 回复Ta


wahaha_a 2017-12-26 15:06:34

谢谢分享！

0 回复Ta


站着洗澡 2017-12-28 13:38:14

@hades 我复制来了

2014年考，现在估计改了题库，知识考点可作为参考。

CISSP考题回忆
注：打斜的为我考试所选答案，不一定为标准答案。
1、
250题里面有的（不保证100%一样，但是知识点是一样的，不要记答案，顺序会变）：2、42、68、91、97、104、117、127、128、130、147、153、156、169、1
2、 150题里面的：47、80、107（选项里面的双重网关主机变为了单宿主机）、142、144
3、 TCP/IP模型的应用层对应OSI模型的应用层和？
a) 会话层、表现层
b) 传输层、会话层
c) 表现层、数据链路层
d) 表现层、传输层

4、 路由器工作在OSI模型的哪个层之间？
a) 数据链路层和表现层
b) 传输层和会话层
c) 网络层和会话层
d) 网络层和传输层

5、 功能最简单的防火墙是哪种类型？
a) 包过滤防火墙
b) 电路代理防火墙
c) 应用代理防火墙
d) 状态监测防火墙

6、 能够应用在可能存在利益冲突的模型是？
a) BLP
b) Biba
c) Brew and Nash
d) CW

7、 下列哪项符合CISSP道德规范？
A、 客户要求低于CISSP道德规范，CISSP提供高于CISSP道德规范的服务
B、 客户要求高于CISSP道德规范，CISSP提供高于CISSP道德规范的服务
C、 客户要求近似CISSP道德规范，CISSP提供CISSP道德规范的服务
D、 客户要求高于CISSP道德规范，CISSP提供低于CISSP道德规范的服务

8、 向密码中"加盐Salts"是为了什么？
A散列hash
B忘记了
C字典攻击
D忘记了

9、 什么样的加密技术使得信息存在这一事实都被隐藏了？
A、 隐写术
10、 员工离职有2题，
离职后账号怎么办？禁用、保留、降权
自愿离职：交回收缴令牌、门卡等，账号等物

11、 ECC相比RSA的好处？
A、 快
B、 密钥长
C、 有限域的离散对数
D、 更安全

12、 The company has written a policy banning wireless networks、 During a quarterly audit a wireless network has been located in the organization、
What is the next step for the organization?
公司写了一个策略来禁用无线网络。在季度审计中发现该组织存在一个无线网络。那么组织的下一步应该做什么？
A、 Report details of the finding to law enforcement
向法律部门报告发现的细节
B、 Remove the wireless network
移除这个无线网络
C、 Reprimand users for the wireless deployment
谴责用户部署了无线网络
D、 Preserve the wireless network for prosecution
为了起诉保留无线网络

13、 下面哪个是使用纵深防御原则的潜在缺陷？
A、增加了系统复杂性
B、增加了组件的故障率
C、需要冗余的组件
D、较低的入侵检测性能

14、 审计师在执行一次合规性审计，申请查看系统中加密的密码，以验证密码是否符合政策。 下列哪项是对审计师最好的回应？
A、 Provide the encrypted passwords and analysis tools to the auditor for analysis、
提供加密的密码和分析工具给审计师进行分析
B、 Analyze the encrypted passwords for the auditor and show them the results、
为审计师分析加密的密码，并给他们看结果
C、 Demonstrate that non-compliant passwords cannot be created in the system、
证明不符合政策的密码不能在系统里创建。
D、 Demonstrate that non-compliant passwords cannot be encrypted in the system、
证明不符合政策的密码不能在系统里加密。

15、 一个维护服务，提供了计算机和相关外设的场所，只差最近一次备份数据，最好形容为
A、 hot site、 热站
B、 cold site、 冷站
C、 warm site、 温站
D、 reciprocal site、 互惠站点

16、 与硬件加密相比，软件加密一般
A、 less expensive and faster、 更便宜、更快
B、 less expensive and slower、 更便宜、更慢
C、 more expensive and faster、 更贵、更快
D、 more expensive and slower、 更贵、更慢

17、 视网膜扫描生物识别装置的物理特性是什么？
A、 The amount of light reaching the retina
到达视网膜的光的数量
B、 The amount of light reflected by the retina
视网膜反射的光的数量
C、 The size, curvature, and shape of the retina
视网膜的大小、曲率和形状
D、 The pattern of blood vessels at the back of the eye
眼睛后面的血管的图案

18、 为什么国际数据传输是比较复杂的？
A、 Some nations subscribe to international conventions、
一些国际签署了国际公约
B、 Rights of a nation in a jurisdiction are enforceable in all jurisdictions、
一个国家司法的权限在所有司法管辖区执行
C、 Patent, copyright, and trade secret laws are not standardized、
专利、版权和商业秘密法律不是标准的
D、 Rights of a nation to enforce in one jurisdiction apply in all jurisdictions、
一个国家在一个司法管辖区执行的权利应用到所有管辖区

19、 下面哪个是检查时间/使用时间（TOC/TOU）问题的实例？
A、 A user whose profile has been revoked logs on using the password of a valid user of the system、
已经被撤销配置的用户使用系统有效用户的密码来登陆

B、 A user logs on with a valid profile which is revoked without termination of the session、
用户使用一个正确的配置来登陆，该配置已经撤销，但没有终结会话；
C、 A user session is terminated immediately after the user profile is revoked、
用户的配置撤销后，用户的会话立即终止；
D、 A user session is not validated until after the log on、
用户会话没有验证，知道登陆以后

User	Clearance	File	Label
A	Public	1	Public
B	Sensitive	2	Sensitive
C	Secret	3	Secret
D	Top Secret	4	Top Secret

20、 能够拥有最小写权限的用户是？ABCD

21、 下面哪个是正确的？
A、 C和D能够共享文件1和2
B、 A和B能够共享文件3和4
C、 B和C能够共享文件2和3
D、 A和C能够共享文件1和2

23、B创建了3文件，什么权限可以看？Secret和Top Secret

22、 4个人使用对称密钥算法通信，一共需要多少个secret key
A、 2
B、 4
C、 6
D、 8

23、 安全审计员发现了企业内部有一个人和外部犯罪团伙勾结进行犯罪，问审计员下一步应该做什么：
C：联系人力资源部；
D：向管理部门汇报；
A\B选项忘了

24、 WEP的特点？a强制B导出c忘记了D共享

25、 谁来维持认证？
(1)项目经理
（2）证书内审员
（3）安全人员
（4）认证评审机构

26、
安全经理要实施一项防泄密的保护措施年费用是2、5万美元。被保护的秘密价值100万美元，被泄密的概率为0、1，损失因子是0、4。问2年以后这个部门的预算成本是
， 我选13万美元

27、 WTO中规定计算机软件和以下哪个有一样的保护
a) 工艺设计
b) 科学发现
c) 文学创作
d) 艺术作品

28、 萨拉米技术是哪种
（1）从大量电子账户里将小数量的电子账户金额转移
（2）从电子账户里用物理机制截取
（3）从电子账户里自动地截取一个或多个字段

29、 安全委会的职责
（1）督导
（2）提示所有者
（3）建议
（4）合规

30、 沙箱
（1）限制网上下载的代码访问下一层
（2）禁止网上下载的代码访问下一个层
（3）为网上下载的代码提供可信计算环境

31、 在限定的区间里面执行代码什么的，是什么技术？1）沙箱

32、 逻辑访问控制，结合哪个最有效？
（1）由安全人员负责维护

（2）安全令牌一起用

33、 ESP作用，比AH多个保密功能

34、 一个访问控制系统，能够抗playback攻击并且采用plaintext secret传输，问是什么认证方法。

35、 还有一道场景题，好像是公司新来了个安全顾问，打算提高公司的安全防护水平，但是公司预算有限。那么他首先打算怎么做？
A。和公司高层开会讨论
B。设置安全基线
C。做预算表，考虑安全和成本的平衡
D。制定公司安全策略

36、 好像是公司的安全顾问，打算提换防火墙，但是公司预算有限，5年后可以减少成本投入，如果要使用新的防火墙，那么他打算怎么说服管理层？
A风险
B忘记了
C年损失预期
D单一预期损失

37、 价值100美元的资产被盗的概率是0、5，价值500美元的资产被盗的概率是0、1。问总的预估损失是多少？
A、600
B、100
C、55
D、5

38、 关于非法闯入的物理安全，哪个最有效
a) 保安或者警察，快速逮捕入侵者
b) 灯光大亮，吓退入侵者
c) 用警报吓退入侵者
不记得了

39、 服务器接交换机的端口1，笔记本接交换机的端口23。问笔记本怎样能截获服务器的信息。
e) 端口生成(port spanning)
f) 端口复制(port copying)
g) 端口绑定（port binding）
h) 端口汇聚（port trunk）

40、 S-http陈述对的？
A、对称和非对称加密
B、文本加密传输（telnet、ftp等）
C、3des加密

41、 Ppp使用了什么协议？lcp 、ptp、还有忘记了

42、 插入了script是什么攻击？注入、XSS、

43、 使用了16进制转换的是什么攻击？XSS

44、 Kerberos使用什么加密？非对称

45、 CA的一部分？pki

46、 以下什么工作需要几个人分开干（职责分离）？不同的XXXX、忘记选项了，我选了的是不同的数据写入和记录员

47、 独立测试比自主测试好处？客观、主观、重要、

48、 大量无线网络怎么监测？所有信道、每个无线路由器、高频率使用的无线

49、 在网络中大量用户分配密钥（对称）有什么影响？占用带宽、服务器资源大量占用变慢

50、 什么违背了引用监视器的问题？客体访问主题、进程直接访问客体、监视器访问客体

51、 认可和认证有几题，不太清楚了，认可什么，认证什么，怎么获得，要熟悉2者的关系和区别

52、 采用了身份验证、身份识别，网络传输加密，问是属于以下的什么？机密性、可用性、纵深防御、完整性

53、 Arp攻击？广播地址、IP、

54、 版本控制是为了什么？报告、程序、输出

55、 公司产品通过CC为了什么？评估目标、安全目标、

56、 Eap比ah多了什么？加密

57、 PPP和L2TP，chap、ssl、tsl，要熟悉和区别。记得有题问到了，什么可以使用证书？我选了SSL和ppp

58、 给你一个算法，要能区别什么是对称加密和非对称加密。

59、 配置管理基本都是在变更那块考。

60、 业务连续性都是知识点的题，主要还是在灾难恢复考的比较多。

61、 WIPO的作用？A，取代本国的专利 B延长时间 C忘记 D，简化……申请的标准流程

62、 Mac，dac，角色访问控制，要分清楚，要注意看题，看清楚是MAC还是DAC

63、 硬盘消磁、重写、覆盖区别，要知道销毁数据怎么做才有用。

64、 数据删除什么最可能没有用（就是还有可能恢复）？覆盖几次、重写、消磁、销毁

65、 不要全看英文，就例如可用性翻译为可获得性，差点就选错了，看了英文才是Availability。

多看真题

0 回复Ta

果果oprah123 2019-02-20 17:17:44

感谢分享

0 回复Ta

EviLAsH 2019-10-14 13:33:12

楼主 网盘链接失效了 请问有最新的吗

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板