



INSTITUTE FOR SECURITY AND OPEN
METHODOLOGIES

JACK

THE JACK OF ALL TRADES SECURITY TESTING TRAINING SUPPLEMENT (CHINESE)

Created by Pete Herzog

CURRENT VERSION:	jack.chn.1.0. 翻译者: 何晔(workflow@alum.swarthmore.edu)
NOTES:	Version Information The JAT Training program is currently only in this form but will be developed further to exist as an online tutorial as well. The HTML training will take place as a form in which the SUBMIT button will return to you a copy of all your answers and the top answers collected from each section. Future versions will also include parallels to the OSSTMM and notes for trainers. More trade scenarios to be added to cover more elements from the manual.
CHANGES:	
DATE OF CURRENT VERSION:	March 19 2001
DATE OF ORIGINAL VERSION:	

THE JACK OF ALL TRADES SECURITY TESTING TRAINING SUPPLEMENT by [Pete Herzog](#)

全能网络安全测试规范附属培训材料

现版本: jack.chn.1.0.x

现版本日期: 2001年3月26日, 周一

初版日期: 2001年3月19日, 周一

作者: Pete Herzog

© 2000 - 2003; 要贡献者:

鸣谢: Marta Barceló

Peter Vincent Herzog

版权所有, 2001年。在GNU公共版权保护下可供免费传播。本文件中所有内容未经作者明确同意不得修改或出售。

版本信息

全能网络安全培训法目前只以本形式存在, 但以后会有在线版本出版。HTML版本将会有个提交 (SUBMIT) 键, 按此键会把你的答案以及其他学员对各章节的答案的最高选择反馈给你。今后的版本还会包括与规范手册平行的问题, 以及专供培训教师的注解。© 2000 - 2003; 了能够更全面地配合规范手册, 我会加入更多的问题。

介绍

“全能”是一本辅助培训手册, 专供培训新员工成© 2000 - 2003; 合格的网络安全测试员。它基于“开放代码安全测试规范手册”。这项培训有益于帮助网络安全行业人员学习非常规性的思维, 从而领悟到如何从不同角度来应用他们的所知。这对于网络安全是有益的, 因© 2000 - 2003; 安全测试人员必须象黑客一般地思维, 同时又必须保持行© 2000 - 2003; 专业化。

开始

在本项培训中, 学员必须假想成© 2000 - 2003; 如邮差或医生的其他行业人士, 并且回答相应的问题。在这些行业中, 你必须描述如何完成每一项任务。总共有十种情景, 每一种包括四道题目。学员必须回答所有问题, 且答案应该简短而切中要害。请按给出情景的次序回答, 而不要跳题。不真实的答案是无效的。请勿必用单句来回答。每一题的时间不得超过十分钟。

这不应该按照心理测试来对待。每一题回答完毕后, 培训教师应该公布学员们的答案, 并就此展开讨论。答案好坏及其原因都应该讨论。最后一题的讨论之后, 教师应该就所有这些问题与网络安全的并行关系再次进行讨论。

情景

每一种情景的设计都是© 2000 - 2003; 了使学员更清晰地了解网络安全测试。有的与网络安全直接相关, 有些则是© 2000 - 2003; 了配合规范手册的教学。

情景一: 电工

你是一名电工。在你前面是一盏吊在天花板上的灯，在你后面是墙上的电灯开关。灯目前开着。

1. 列出10种关灯方式。
2. 列出能发光的灯的10个组成部分。
3. 列出10种方式来判别灯是关着的。
4. 列出10种防止别人关灯的方法。

情景二：邮差

你是一家独立经营的快递公司的一名邮差。你有一份书本大小的邮件要送。

1. 列出10种判别出收件人的方法。
2. 列出10种会令你无法递送这封邮件的东西。
3. 列出10种你要递送这封邮件的原因。
4. 列出10种判别出发件人的方法。

情景三：唱片店老板

你酷爱音乐，并且由此拥有一家独立经营的唱片店。该店成功与否取决于同样酷爱音乐的顾客们。

1. 列出10种把店中唱片分类的方法。
2. 列出10种判别一个可能成 2000 - 20036; 顾客的人对音乐品味的方法。
3. 列出10种唱片防盗的方法。
4. 列出10种令人不愿购买你唱片的的东西。

情景四：医生

你是一名有执照的外科医生。一个没有反应的男孩被送到你的诊所。

1. 列出10种不经意地处理这个男孩而可能引起的危险。
2. 列出10种令这个男孩有所反映的方法。
3. 列出10种安全地检查这个男孩的预防措施。
4. 列出10种找出这个男孩病症的方法。

情景五：士兵

你是一名战争中的全副武装的士兵。你驻扎在跨越峡谷的唯一的桥梁。

1. 列出10种准备敌人来犯的方法。
2. 列出10种不让敌人过桥的方法。
3. 列出10种分辨敌人与友好过桥人员的方法。
4. 列出10种敌人一旦成功过桥后能引起的麻烦。

情景六：安检员

你是一名有执照的安全检察员，在一家独立的行业安全协会供职。你来到一家大工厂检查其机器设备的安全性，因 2000 - 20036; 已经发生了多起事故。

1. 列出10个问题来问这家工厂的工头。
2. 列出10种工厂员工由于最近事故增加而可能产生的忧虑。
3. 列出10种可以提高这家工厂生产安全度的变化。
4. 列出10种工厂员工对实施以上变化而可能产生的疑虑。

情景七：技工

你是一家连锁汽车修理行的技工。有人要你就一辆二手车提供你的专家意见，因 2000 - 20036; 他在考虑购买这辆车。

1. 列出10个给卖方的问题。

2. 列出10个该车上应该受检查的零部件。
3. 列出10个你的这种服务有益于卖方的理由。
4. 列出10个另一个技工的专家意见可能与你的不同的原因。

情景八：电脑服务中心支持人员

你在一家大公司内部的电脑服务中心工作，通过电话支持全球员工使用电脑。你工作在服务中心第一线，这意味着你首先收到所有关于电脑支持的电话。

1. 问10个可能帮助你诊断的问题。
2. 列出10个可能帮助你解决问题的资源。
3. 列出10种与你通电话的员工对接受你的建议可能产生的疑虑。
4. 列出10种使你能提供最佳服务的方法。

情景九：建筑检查员

你是纽约市一名有执照的桥梁和房屋检查员。你现在要检查布鲁克林大桥，提出维修建议。

1. 列出10种纽约市府可能对你的桥梁检查工作所产生的疑虑。
2. 列出大桥中10个你可能检查的部位。
3. 列出10种你对封闭大桥进行维修可能产生的疑虑。
4. 列出10种你在封闭大桥前会做的准备工作。

情景十：小偷

你专偷窃钻石。目前你在夜间独自行动。

1. 列出10种选择珠宝店目标的方法。
2. 列出10种可能令你无能© 2000 - 20036;力的防盗措施。
3. 列出10件你在行窃时© 2000 - 20036;避免落网可能要做的事。
4. 列出10种能令你每次行动的收入得到增加的方式。

作者：Pete Herzog (pete@isecom.org)

翻译者：何晔(workflow@alum.swarthmore.edu)