



INSTITUTE FOR SECURITY AND OPEN  
METHODOLOGIES

# JACK

## THE JACK OF ALL TRADES SECURITY TESTING TRAINING SUPPLEMENT

Created by Pete Herzog

<b>CURRENT VERSION:</b>	1.0.
<b>NOTES:</b>	<b>Version Information</b> 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.
<b>CHANGES:</b>	
<b>DATE OF CURRENT VERSION:</b>	March 19 2001
<b>DATE OF ORIGINAL VERSION:</b>	

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

### Introduction

JAT is a supplementary training manual for testing and training new employees to be security testers. It is based on the Open Source Security Testing Methodology Manual. This training has the benefit of teaching security professionals to think "outside the box" and to learn to use their knowledge in different ways. This is beneficial in security testing where the tester is required to think like a hacker and act like a professional.

### Getting Started

In this training program the trainee is required to assume different professions from postman to doctor and to answer the questions accordingly. Within these professions you are required to describe methods for performing a task. There are ten different trade scenarios. Each scenario has 4 questions. The trainee is required to fill all the blanks. The answers should be brief and to the point. The scenarios should be accomplished in order. Do not skip ahead. Untrue answers are not valid. Keep all answers to single sentences. There is a maximum of 10 minutes per question.

This should not be treated like some sort of psych analysis. After each question, the trainer should open discussion on the answers and list the answers for all to see. Good and bad answers should be discussed and why. After the last discussion, the trainer is expected to discuss the parallels between the questions and Internet security.

## Scenarios

Each scenario is designed to discuss security in a way that makes security testing clear to the trainee. Whether it be what needs to be tested or how should be taught in conjunction with the OSSTMM.

### Scenario One - Electrician

You are an electrician. In front of you is a light hanging from the ceiling and behind you is a light switch on the wall. The light is currently on.

1. List 10 ways to turn off the light.
2. List 10 components of a functioning light.
3. List 10 ways to tell if the light is off.
4. List 10 ways to prevent someone from being able to turn off the light.

### Scenario Two - Postman

You are a postal carrier for an independent express postal service. You have a book-sized package to deliver.

1. List 10 ways to identify the RECEIVER of the package.
2. List 10 things which would stop you from delivering the package.
3. List 10 reasons for delivering the package at all.

4. List 10 ways to identify the SENDER of the package.

### Scenario Three - Record Store Owner

You own an independent record store which grew out of your intense fascination with music. The success of your store depends on your customers who are also music enthusiasts.

1. List 10 ways to categorize the records in the store.
2. List 10 ways to identify a potential customer's musical tastes.
3. List 10 ways to protect your records from theft.
4. List 10 things that would influence a customer NOT to buy from you.

### Scenario Four - Doctor

You are a licensed doctor of general medicine. An unresponsive boy is brought to your office.

1. List 10 dangers of handling the boy without proper precautions.
2. List 10 ways to make the boy respond.
3. List 10 precautions you can take to examine the boy safely.
4. List 10 ways to discover the boy's illness.

### Scenario Five - Soldier

You are a soldier in full field gear during war time. You are stationed at the only bridge which crosses over the gorge.

1. List 10 ways to prepare for the coming enemy.
2. List 10 ways to prevent the enemy from crossing the bridge.
3. List 10 ways to discern friendly bridge users from the enemy.
4. List 10 problems the enemy could cause if they crossed the bridge.

### Scenario Six - Safety Inspector

You are a licensed safety inspector for an independent occupational safety consortium. You have been brought to a large factory to review the safety of their machines due to a high number of accidents.

1. List 10 questions you would ask the foremen of this factory.
2. List 10 concerns the employees may have with the current rise in accidents.
3. List 10 changes which would make the factory a safer place to work.
4. List 10 concerns the employees may have with the implemented changes.

### Scenario Seven - Mechanic

You are a mechanic at one of a chain of general automotive repair garages. A car is brought to you by a person interested in purchasing it second-hand and would like to get an expert opinion about it.

1. List 10 questions you would ask the seller of the car.

2. List 10 parts of the car which should be inspected.
3. List 10 reasons why this service helps the seller.
4. List 10 reasons why the buyer may receive a different expert opinion somewhere else.

### **Scenario Eight - Computer Help Desk Support Person**

You work telephone help desk support for a large corporation dedicated to assisting its employees with support questions worldwide. You are the front line of defense which means you receive all support matters.

1. List 10 questions you may ask to diagnose the problem.
2. List 10 resources you could use to solve the problem.
3. List 10 concerns the caller may have with following your advice.
4. List 10 ways you can assure better service.

### **Scenario Nine - Building Inspector**

You are a accredited bridge and building inspector for New York City. Your job is to assess the Brooklyn Bridge for repairs.

1. List 10 concerns the city may have with this bridge inspection.
2. List 10 areas of the bridge you may assess for safety.
3. List 10 concerns you may have with shutting down this bridge for repair.
4. List 10 preparations you will have to make before shutting down the bridge.

### **Scenario Ten - Thief**

You are a diamond thief. You currently work independently at night.

1. List 10 ways to choose the best diamond store to rob.
2. List 10 security mechanisms which you may have to avoid.
3. List 10 things you will have to do to avoid detection during the job.
4. List 10 ways to increase the amount of money you make from each job.