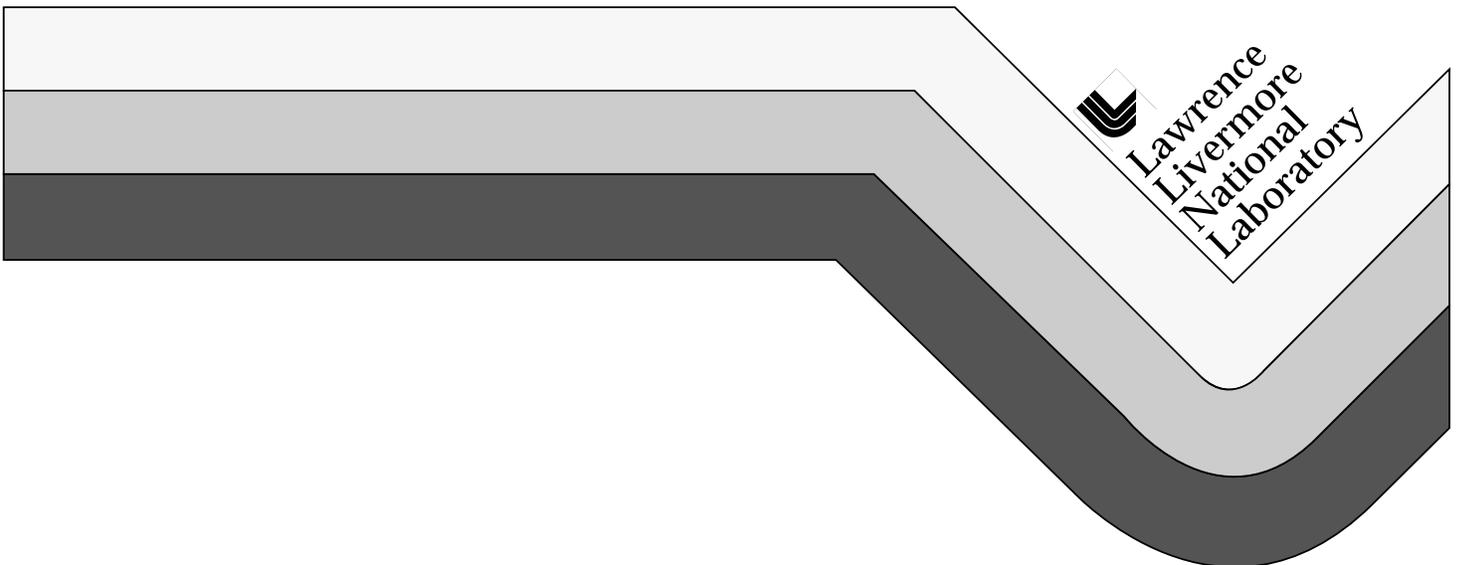


# User's Guide for the IEBT Application

Tony Bartoletti

April 30, 1999



#### DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

## Contents

<b>1.</b>	<b>What is IEFT?</b> .....	<b>4</b>
<b>2.</b>	<b>What purpose does the IEFT application serve?</b> .....	<b>5</b>
<b>3.</b>	<b>How do I get started?</b> .....	<b>6</b>
<b>3.1</b>	<b>System Requirements</b> .....	<b>6</b>
<b>3.2</b>	<b>Installation</b> .....	<b>6</b>
<b>4.</b>	<b>Operation</b> .....	<b>8</b>
<b>4.1</b>	<b>Launching IEFT</b> .....	<b>8</b>
<b>4.2</b>	<b>IEFT Scenarios</b> .....	<b>8</b>
<b>4.2.1</b>	<b>Entering a User Name</b> .....	<b>8</b>
<b>4.2.2</b>	<b>Beginning a Scenario</b> .....	<b>9</b>
<b>4.2.3</b>	<b>Scenario Navigation</b> .....	<b>9</b>
<b>4.2.4</b>	<b>Scenario Objectives</b> .....	<b>10</b>
<b>4.2.5</b>	<b>Tools of the Trade</b> .....	<b>10</b>
<b>4.2.6</b>	<b>Measures of Success</b> .....	<b>11</b>

## 1. What is IEBT?

INFOSEC Experience-Based Training (IEBT) is a simulation and modeling approach to education in the arena of information security issues and its application to system-specific operations.

The IEBT philosophy is that "Experience is the Best Teacher".

This approach to computer-based training aims to bridge the gap between unappealing "read the text, answer the questions" types of training (largely a test of short-term memory), and the far more costly, time-consuming and inconvenient "real hardware" laboratory experience. Simulation and modeling supports this bridge by allowing the critical or salient features to be exercised while avoiding those aspects of a real world experience unrelated to the training goal.

IEBT intends to demonstrate that even a solitary (non-classroom) training program can be

- Engaging, challenging and rewarding (i.e., enjoyable)

Education is something exciting and recreational that we can look forward to, rather than a dull chore we would just as soon avoid where possible. Being receptive to the experience enhances the ability to learn.

- Immersive (exercise more than short-term memory)

What we say we would do, or think we would do in a particular situation is not always what we actually do when the real situation presents itself. Real learning, more than memorization, involves understanding and appreciating the interaction and dependencies among the elements of a training experience.

- Cost-effective (flexible, easily deployed and conveniently operated)

Simulation software can be designed to run on relatively low-cost platforms, yet simulate the features of an expensive and complex system targeted for training. It can be easily deployed, and operated at the convenience of the trainee. In addition, a well designed, data-driven simulation engine can facilitate the development of new training targets and requirements without requiring significant retooling of the underlying software.

We hope you will enjoy giving this IEBT application a test drive, and that you will see the potential that experience-based simulation holds in providing effective INFOSEC training.

## **2. What purpose does the IEBT application serve?**

The scenario packaged with the IEBT 1.0 release is intended to give beginner and intermediate level system administrators the experience of detecting and dealing with security events, both innocent and malicious. The Scenario Experience Engine employs a fair degree of open-ended, statistical and deterministic modeling of the cause-and-effect relationships among information system variables and decisions. It is also largely data-driven, and can be quickly reconfigured by the developers to exercise different areas of domain knowledge, or vary the focus between general issues and specific system details.

For the purposes of prototype demonstration, we have included the opening chapters of a "System Administrator's" scenario exercise.

Given the time and resources available, we felt it more important to exercise a variety of potential training elements, rather than focus upon faithfulness to a particular computer operating system or upon a completely accurate depiction of particular system security details. For this reason, you will see a "system" that includes both NT and UNIX features and terminology. Also, the amount of detail and accuracy provided in operating or configuring system functions is intended to convey a sense of what is possible to emulate with a tool of this kind.

Future IEBT versions will exercise a greater breadth of material, as well as provide a more detailed and accurate depiction of the features of particular systems and system administration tasks. In addition, we intend to provide a "scenario debriefing" mode that will point out to you what "really happened" in the scenario, how your actions affected the results, and what you can do to improve your performance.

### **We need your feedback!**

You can help to influence the direction IEBT takes in scenario development. Please feel free to write to us with your suggestion or critique of the product. In particular, let us know the changes or additions that you feel would help to make this product of service to your individual training requirements.

Please write to [azb@llnl.gov](mailto:azb@llnl.gov) (Tony Bartoletti) regarding the IEBT development effort.

### 3. How do I get started?

#### 3.1 System Requirements

The IEBT application is designed to operate on most Windows-NT and Windows 95 systems that support multimedia presentations. We consider the minimum system requirements for effective IEBT operation to be:

- CPU:** A i486 or Pentium-strength processor is recommended
- MEMORY:** 16 MB system RAM (32+ MB preferred)
- DISK:** 180 MB free disk space is required during installation.  
(60 MB free disk space required for routine use)
- SOUND:** A "SoundBlaster" or equivalent sound card
- GRAPHICS:** Minimum SVGA 640x480 display resolution (1024x768 preferred)  
with standard graphics accelerator card.

The above features are standard on most contemporary PC systems.

**Note:** In order to ensure that automatically-generated text displayed correctly, it is advised that you set your system font-size selection to "Small Fonts" and set the system color-depth to 8-bit color (256 colors). You can do this by navigating to the "Start: Settings: Control Panel" folder, selecting the "Display" icon, and then selecting the tab labeled "Settings". On this panel you find a field called "Font-Size" that allows you to switch between "Large Fonts" and "Small Fonts". Please select "Small Fonts" to ensure that all the scenario text displays properly. Also select "8-bit" or 256 colors in the color-depth selection menu located on the same screen. (On some systems, you may need to reboot in order to have these settings take effect.)

#### 3.2 Installation

The IEBT application is packaged in a self contained executable file named "IEBT-Install.exe". Simply invoke the file to begin installation.

The InstallShield system will first unpack the IEBT components in a temporary location. By default, this location is <current drive>:\TEMP\IEBT-Unpack. InstallShield will then proceed to complete the installation, and you will have an opportunity to designate the final location for the IEBT product (default is <current drive>:\Program Files\IEBT). After installation is complete, you may delete the file "IEBT-Install.exe" and the

temporary folder "TEMP\IEBT-Unpack" along with its contents, in order to recover about 100 MB disk space.

A complete installation is comprised of the "IEBT.exe" product executable, this document, and a parallel folder called "Data" which contains the files that define the selected scenarios and allow you to save your progress.

No desktop icon is created. You must use your file manager (Explorer or equivalent) to navigate to the "Program Files\IEBT" folder in order to launch "IEBT.exe".

## **4. Operation**

### **4.1 Launching IEBT**

To launch IEBT, simply navigate to the folder containing the "IEBT.exe" file, and double-click on the entry.

Within a few moments, you should see the IEBT Introductory movie sequence. This one-minute movie sets the tone for the IEBT experience. You can interrupt the movie at any time by clicking on it with the mouse. The movie will fade to the IEBT "Main Menu". The main menu allows you to navigate to four areas, three of which ("Intro", "Help", and "Credits") are purely informational.

The fourth area, labeled "Start", will introduce a screen for you to enter a user name and access the available scenarios. Details on scenario operation are contained below, and are also available through the IEBT main menu "Help" selection.

### **4.2 IEBT Scenarios**

[NOTE: The following pages describe the contents of the IEBT Help section.]

The IEBT Help Pages are divided into several sections

- 4.2.1 Entering a user name
- 4.2.2 Beginning a scenario
- 4.2.3 Scenario Navigation
- 4.2.4 Scenario Objectives
- 4.2.5 Tools of the Trade
- 4.2.6 Measures of Success
- 4.2.7 Exiting a scenario

#### **4.2.1 Entering a user name**

When you are ready to begin a scenario, press the "Start" icon on the main screen.

You will be prompted to enter a user name. This name will be used in two ways. First, it will define the folder in which you can save and retrieve the progress of your scenarios. It is also the name of the "character" you play in the scenario.

For these reasons, you are limited to an alphabetic user name containing no white-space, and a maximum of 8 characters.

### **4.2.2 Beginning a Scenario**

Once you have entered a user name, you will be presented with the scenarios that are available to exercise. The upper window contains scenarios that you may start from the beginning. The lower window contains scenarios in which progress has been saved. If this is the first time you have used this IEFT program, the lower window should be empty.

To start a scenario from the beginning, simply double-click on an entry from the top window. To resume a saved scenario, double-click on an entry in the lower window.

Note: When you select a "Saved" scenario, you will also have the option to delete the saved scenario.

In the included SysManager scenario, you are first greeted with a letter. Read the letter carefully to understand what your management expects of you. You will then have a one-time opportunity to set the scenario run-speed. This setting determines how quickly the daylight hours pass. (Note: Time always passes quickly in the evening hours.)

You will soon find yourself in the office, where (at present) you will spend all of your time trying to maintain your firm's file server. There are several "active elements" in the office. You can click on the phone to place outgoing calls or answer incoming calls. You can click on the timepiece to see a log of all of your calls (even those that you do not pick up.) You should examine the "Operation Manual" on the desktop, as it will answer many of the questions you may have about your role in the scenario, and how to accomplish the many tasks you will need to perform. Most important, you can click on the "system console" monitor to explore the system you are tasked to manage.

In the SysManager scenario, the simulated file server is "down" when you first appear in the office. On the computer tower you will see a power button. This button serves as the main power switch to the server. You will need to power the system up, and then keep it running smoothly while familiarizing yourself with its features.

NOTE: The only way to recover from a "BlueScreen" or system crash is by powering the system off and then back on again.

You may save your progress at any time by pressing the "Save and Continue" button at the top of the screen. Also, anytime you exit the scenario, you will be given an opportunity to save your progress, and even to modify the "save" name in order to effect progress branching.

### **4.2.3 Scenario Navigation**

When a scenario is run from the beginning, you will be given the opportunity to set the RunSpeed. The speed chosen will thereafter remain set at the selected value.

Note: Time always passes rapidly at night!

While in the scenario, there will be a menu bar displayed at the top of the screen. This bar will contain the following options:

**Preferences** - Allows the adjustment of background sound/volume

**Save & Continue** - Force your progress to disk, (just to be safe)

**Exit Scenario** - Halts the scenario and takes you to the Save/SaveAs screen

**View Progress** - Displays numerous stats to help you chart your progress

**Pause** - Halts progress of time, and disables mouse-clicks except for "Resume"

Note: The scenario is also "Paused" in the Preferences or View Progress screens.

#### **4.2.4 Scenario Objectives**

The central objective of the INFOSEC Experience-Based Training Scenarios is to find and exercise the "best path" as you balance two competing needs. You are charged with the responsibility of maintaining a system or network. You need to keep this system active and available in order to support the greatest number of users. But you must also implement measures to improve the security of that system against both insider and outsider attacks.

In general, the more users you try to support, the more frequent the attacks and other security-related events become. And if you do not respond appropriately to mitigate the ill-effects of a recent "hack", you may find your problems escalate to more damaging or insidious forms of attack. In addition to attack mitigation, you must also exercise the proper and timely reporting of significant security events.

#### **4.2.5 Tools of the Trade**

There are a wide variety of tools you may employ in order to perform your tasks.

##### **The Telephone:**

The phone in your office allows you to communicate with your staff, your security office and others. You can often learn about ongoing events by receiving or placing calls, and you will need to use the phone to report suspect events. Also, you may receive calls from staff seeking your expert guidance on various issues.

##### **The Date/Time:**

The clock in the office serves more than to tell you the current day and time. Double-click on the icon, and a screen will appear that allows you to review every telephone conversation you have had during the scenario. If you "miss" a call (if you do not pick up in time) then you can use this feature to see your "voice mail".

## **The Operations Manual:**

Clicking on the "Operations Manual" on the desk in your office will bring up a screen containing online help, and other guidance you may need during the scenario. The text is divided into four areas:

- Overview and Objectives
- Policy
- Systems
- Commands

## **The Computer:**

The greatest variety of "tools" is available on the computer itself. These tools include:

- Specification of System Run-Level, Maximum Concurrent Users, and Auditing Mode.
- Configuration of User Accounts and Network Services. Monitor active processes.
- Installation of system patches and various security services.
- Perform system backups, restore from backup, and re-install OS (if all else fails!)

In addition, a "Command-Line Window" allows you to manage a Virtual File System. Among the commands available are:

cat, cd, chgrp, chmod, chown, cp, find, grep, kill, ls, mkdir, more, nslookup, passwd, ps, pwd, sum, touch, uname, and even an (ersatz) "vi".

Examples: Use "chmod" to lock-down important directories and files, and use "sum" and output redirection to record important binary checksums.

### **4.2.6 Measures of Success**

The "View Progress" option will take you to a screen that provides many different ways to chart your progress, as well as inform you of certain critical status values.

#### **Chronograph:**

Time spent in the scenario (sim-time and real-time)

#### **Operational Status:**

System is (Online/Offline) and for how long.

#### **Operational Rating:**

Percent of time system has been "up", and mean number of users supported.

#### **Q/A Score Rating:**

Some of those telephone calls are actually "stealth exams!"

Throughout the scenario, events occur that are labeled Level-1, Level-2, or Level-3 in severity. Level-1 events may represent malicious activity, or may be "innocent" events that produce suspicious symptoms. Level-2 or 3 events are indeed attacks, and must be treated as such.

Events are "Cleared" when their symptoms or damages have been mitigated, and they have been properly reported. Some events may be "self-mitigating", such as receiving a threatening phone call. Level-1 events do not need to be reported.

The scenario "Status" screen shows the number of untreated, mitigated and reported events of each severity level that are active at any given time.

### **The "Bottom-Line":**

In an exercise such as the IEBT scenarios, it is difficult to produce a single measure to represent your overall "score". We have chosen one that almost everyone should be able to relate to -- a paycheck.

For convenience as a metric, you are awarded a "days pay" each night at midnight. The payment begins with a base-salary that is raised in small increments each day, but may contain several large "bonus" awards for high productivity, system up-time, and average number of users supported. However, these bonuses are also reduced when significant open incidents are active.

The scenario "Status" screen will show you the value of your last paycheck, and the total amount earned in this scenario.

(Think you can make \$2000 in the first 5-days? Good luck!)