

# Spider Workshop – Student Handbook

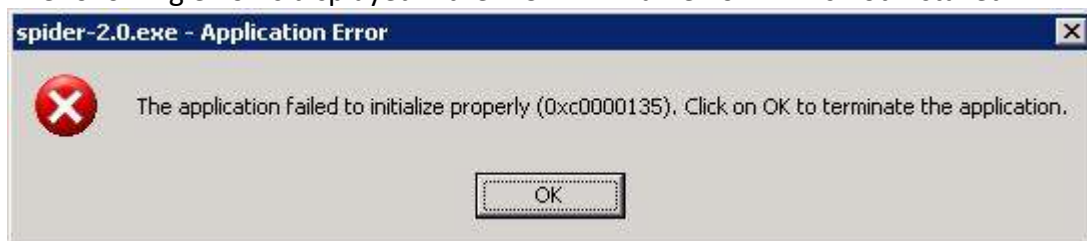
## ***Introduction***

This handbook is provided to supplement the “Spider Documentation for Tier 2” guide. These exercises demonstrate Spider version 2.9.1 and should be run on a Windows XP operating System.

## ***Module 1***

### **Exercise 1 – Checking for Microsoft .NET Framework 1.1 or later**

1. Go to Start and click on Run...
2. Type appwiz.cpl
3. In the “Add or Remove Programs” window, look for Microsoft .NET Framework 1.1 or later
4. If it is not installed, run Windows Update and include the Microsoft .NET Framework 1.1 from the optional updates.
5. The following error is displayed if the MS .NET Framework 1.1 is not installed:



### **Exercise 2 – Installing Spider**

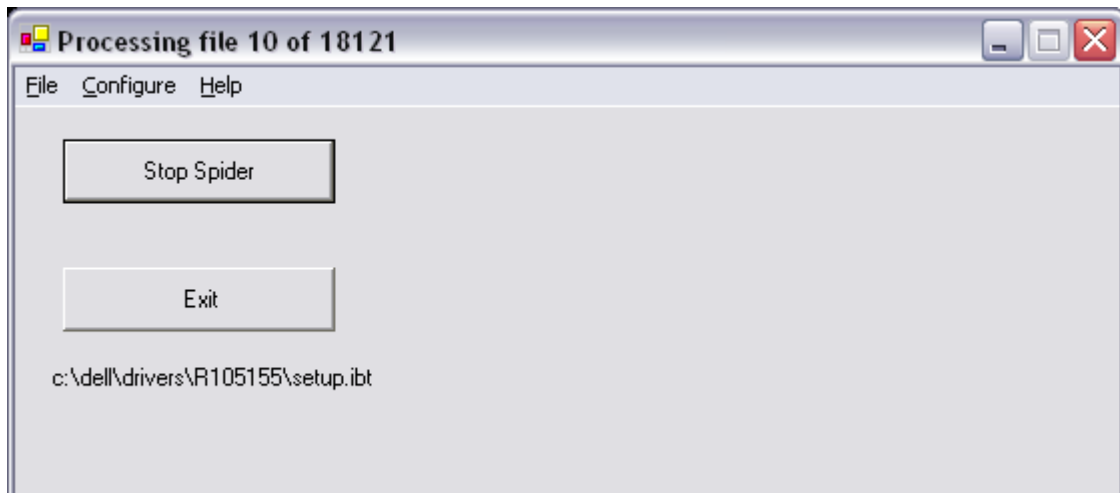
We will be using the repackaged installer available from ITS at <http://www.colorado.edu/its/docs/security/spider>

1. Double click the spider.msi icon
2. Accept all of the default values by clicking next
3. At the end of the installation wizard, click Finish

## ***Module 2***

### **Exercise 1 – Running a Spider Scan from GUI**

1. Go to Start -> Programs (or All Programs) -> Cornell Spider -> Spider
2. Click on “Run Spider”
3. How many files will Spider process? (Hint: check the title bar)



4. Stop Spider by clicking the "Stop Spider" button (which is the same button you clicked to start the scan)

### **Module 3**

#### **Exercise 1 – Configuring Spider for Workshop**

We will now configure Spider to look in a specific directory that will scan fewer files that we can use as examples.

1. With Spider open, go to Configure -> Settings
2. Click on the Files tab
3. In the Directory sub-tab, click the start dir... button
4. Select the D:\privdata directory and click OK
5. Click Save

#### **Exercise 2 – Interpreting the Log**

1. Run Spider again by clicking the "Run Spider" button (note the number of files to process)
2. After Spider is finished scanning, the Spider Log Viewer will appear
3. What types of files appear? What patterns in the names, extensions, and/or locations of the files provides clues to the content of the files?
4. Click the "View Links" button at the bottom of the Spider Log Viewer
5. Click on a link to a file and examine the contents of the file
6. At first glance, can you find the data that Spider found? Is there a likely reason why the document would contain sensitive data? (Hint: is it the type of document that people in your department often use and is it something they might forget they saved?)
7. Close the files and Spider program.

## **Module 4**

### **Exercise 1 – Common Configuration Changes**

This exercise steps through common configuration changes to cut down on false positives and increase the speed of the Spider scan. **Caution:** These steps may decrease the time a scan takes to complete, but you must understand the effect of these changes. Faster Spider scans run a risk of missing sensitive data files. Remember, this tool is to be used in place of manually opening files and searching for sensitive data yourself.

1. Run Spider from the start menu
2. Go to Configure -> Settings
3. In the Files tab and the Directory sub-tab, click Paths to Skip
4. Click Add New
5. Type "C:\WINDOWS" and click OK
6. Click Add New again and type "C:\winnt" and click OK
7. Click Add New again and type "C:\i386" and click OK
8. In the "Paths to Skip" window, click Save
9. Select the Options sub-tab and select "Scan only the first" radio
10. Enter 30kb
11. In the Spider Configuration window, select the Runtime tab
12. Select the "High" radio in the process priority section
13. Select the Logging tab and add "Quick" to the end of the log file name so we can compare the log files
14. In the Spider Configuration window, click Save
15. Run a Spider scan and note the differences in speed and compare the log files
16. Did the scan go faster? Are there any differences in the log files? Did Spider skip any of the files it caught before?

### **Resources**

For more information on Spider from Cornell University:

<http://www.ats.cornell.edu/security/tools/>

For more information on data classification:

<http://www.colorado.edu/its/security/assetinventory/>