



# Module 4 Working with Information Sources Lab

## Student Guide



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

## Lab Introduction

- Open your Lab Student Guide
- Your instructor will guide you through each step



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

### Lab Introduction

You will take two scenarios and answer questions methodically in response to the situations and information for each incident. Once we have completed the exercise, we will discuss the answers so you can learn more from others in the class.

## For Each Scenario

For each question in each scenario, ask:

- Which tools are appropriate for investigating the information presented in this question?
- Would you categorize this information as primary, secondary, or tertiary?
  - Primary: the original source of a vulnerability
  - Secondary: information derived from that primary information or from a security database, article, or journal
  - Tertiary: information derived from secondary information



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

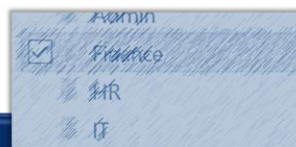
## For Each Scenario

For each question in each scenario, you will also want to think through:

- Which tools are appropriate for investigating the information presented in this question? Refer to the Resource Guide (ask your instructor) and feel free to add tools you like that are not on our list.
- Would you categorize this information as primary, secondary or tertiary? Recall:
  - Primary means the original source of a vulnerability, likely a person or a bulletin.
  - Secondary means information derived from that primary information or from a security database, article or journal.
  - Tertiary means information derived from secondary information, such as a synthesis of a number of articles.

## Scenario 1: Incident Mitigation

- You notice there is a system within your organization that is performing downloads from unusual domains on the Internet
- You find the system is Joan's computer in Finance
- You see that Joan's antivirus and system update processes are not active
- You discover the first download was trafficconverter.biz and from then on there was the strange download every day
- You create a hash of the executable, 59c23e92625559f541b0cbcd46f07dc, and find out that Norton named this worm "Conficker" and Symantec called it "W32.Downadup"



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

### Scenario 1: Incident Mitigation

Here's Scenario 1: You are scanning your network traffic log file and notice there is a system within your organization that is performing downloads from unusual domains on the Internet.

- You look up and find the system is Joan's computer in Finance.
- When you go to Joan's machine you see that her antivirus and system update processes are not active and those are on by default in your organization.
- You look back in the network history and discover the first download was trafficconverter.biz and from then on there was the strange download every day.
- You create a hash of the executable; the hash is 59c23e92625559f541b0cbcd46f07dc. You find out that Norton named this worm "Conficker" and Symantec called it "W32.Downadup."

## Scenario 1 Questions: Incident Mitigation

1. What can you find out from the network traffic log file?
2. How could you determine that it was Joan's machine?
3. Is there any general information on the Web about malware that "disables antivirus software?"
4. What does a search indicate about the [trafficconverter.biz](http://trafficconverter.biz) site?

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

### Scenario 1 Questions: Incident Mitigation

Here are the questions for Scenario 1:

1. What can you find out from the network traffic log file?

---

---

2. How could you determine that it was Joan's machine?

---

---

3. Is there any general information on the Web about malware that "disables antivirus software?"

---

---

4. What does a search indicate about the [trafficconverter.biz](http://trafficconverter.biz) site?

---

---

## Scenario 1 Questions: Incident Mitigation

5. What can you find out from the hash and what does it tell you?
6. What type of file is it and where does it run?
7. What are the vulnerabilities that were exploited?
8. What could have been done to prevent this incident from arising within your organization?
9. What is the family of the malware, e.g., is it a virus, Trojan, or other type of malware?

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

### Scenario 1 Questions: Incident Mitigation

Here are the questions for Scenario 1:

5. What can you find out from the hash and what does it tell you?

---

---

6. What type of file is it and where does it run?

---

---

7. What are the vulnerabilities that were exploited?

---

---

8. What could have been done to prevent this incident from arising within your organization?

---

---

9. What is the family of the malware, e.g., is it a virus, Trojan, or other type of malware?

---

---

## Scenario 1 Questions: Incident Mitigation

10. Are your Windows 7 systems affected?
11. How can you determine whether other machines in your organization are infected?
12. Is this an advanced persistent threat (APT)? How can you tell?
13. What other useful information did you learn along the way that you can share?

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

### Scenario 1 Questions: Incident Mitigation

Here are the questions for Scenario 1:

10. Are your Windows 7 systems affected?

---

---

11. How can you determine whether other machines in your organization are infected?

---

---

12. Is this an advanced persistent threat, or APT? How can you tell?

---

---

13. What other useful information did you learn along the way that you can share?

---

---

## Scenario 1 Question Review

1. What can you find out from the network traffic log file?
2. How could you determine that it was Joan's machine?

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

### Lab Scenario 1 Question Review

Now let's review the answers to your questions.

1. What can you find out from the network traffic log file?
2. How could you determine that it was Joan's machine?

## Scenario 1 Question Review

3. Is there any general information on the Web about malware that “disables antivirus software?”
4. What does a search indicate about the trafficconverter.biz site?

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

### Scenario 1 Question Review

3. Is there any general information on the Web about malware that “disables antivirus software?”
4. What does a search indicate about the trafficconverter.biz site?

## Scenario 1 Question Review

5. What can you find out from the hash and what does it tell you?
6. What type of file is it and where does it run?

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

### Scenario 1 Question Review

5. What can you find out from the hash and what does it tell you?
6. What type of file is it and where does it run?

## **Scenario 1 Question Review**

7. What are the vulnerabilities that were exploited?
8. What could have been done to prevent this incident from arising within your organization?

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

### **Scenario 1 Question Review**

7. What are the vulnerabilities that were exploited?
8. What could have been done to prevent this incident from arising within your organization?

## **Scenario 1 Question Review**

9. What is the family of the malware, e.g., is it a virus, Trojan, or other type of malware?
10. Are your Windows 7 systems affected?

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

### **Scenario 1 Question Review**

9. What is the family of the malware, e.g., is it a virus, Trojan, or other type of malware?
10. Are your Windows 7 systems affected?

## **Scenario 1 Question Review**

11. How can you determine whether other machines in your organization are infected?
12. Is this an advanced persistent threat (APT)?  
How can you tell?

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

### **Scenario 1 Question Review**

11. How can you determine whether other machines in your organization are infected?
12. Is this an advanced persistent threat, or APT? How can you tell?

## **Scenario 1 Question Review**

13. What other useful information did you learn along the way that you can share?

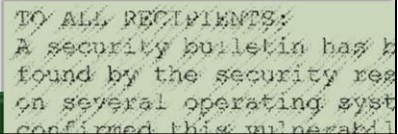
Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

### **Scenario 1 Question Review**

13. What other useful information did you learn along the way that you can share?

## Scenario 2: Vulnerability Research

- Symantec announced an Adobe zero-day was found by the security researcher Kafeine
- Adobe has confirmed this vulnerability and issued a security bulletin
- The infection presents itself to users in two paths:
  - As an Adobe PDF file on spam email attachments that automatically download the malware
  - Through “malvertizing” that pops up on unreliable web pages



TO ALL RECIPIENTS:  
A security bulletin has been  
found by the security researcher  
on several operating systems  
confirmed this vulnerability

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

### Lab Scenario 2 Questions: Vulnerability Research

Here's Scenario 2: You check your security RSS feeds and email lists regularly. Symantec announced an Adobe zero-day was found by the security researcher Kafeine. He completed Proof of Concept testing on several operating systems and browsers.

- (1) Adobe has confirmed this vulnerability, recorded as CVE-2015-0311, and issued a security bulletin.
- (2) The infection presents itself to users in two paths:
  - As an Adobe PDF file on spam email attachments. When you open the attachment, you automatically download the malware.
  - Another way for it to enter your system is through “malvertizing” that pops up on unreliable web pages.

## Scenario 2 Questions: Vulnerability Research

1. What are some advisories of interest, articles, and blog posts that may be used as primary sources of information?
2. If your organization runs Windows 8 and Internet Explorer 10, should you be concerned?
3. According to NIST, what is the CVSS score (out of 10+10+10 or 30)? Does that make you more concerned or less?
4. According to the Adobe Security Bulletin, what are the adverse effects of this malware?
5. Which release or releases are the vulnerable ones?

Training Module 4: Working with Information Sources, Version 1, © 2016 FIRST

### Lab Scenario 2 Questions: Vulnerability Research

Here's are the Scenario 2 questions:

1. What are some advisories of interest, articles, and blog posts that may be used as primary sources of information?

---

---

2. If your organization runs Windows 8 and IE 10, should you be concerned?

---

---

3. According to the U.S. National Institute of Standards and Technology, or NIST, what is the CVSS score (out of 10+10+10 or 30)? Does that make you more concerned or less?

---

---

4. According to the Adobe Security Bulletin, what are the adverse effects of this malware?

---

---

5. Which release or releases are the vulnerable ones?

---

---

## Scenario 2 Questions: Vulnerability Research

6. What are some ways to detect whether a computer has been infected by this vulnerability?
7. What are the two ways your users can get the update?
8. Based on your CSIRT policies, how will you communicate about this incident to your users?
9. What other useful information did you learn along the way that you can share?

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

### Lab Scenario 2 Questions: Vulnerability Research

Here's are the Scenario 2 questions:

6. What are some ways to detect whether a computer has been infected by this vulnerability?

---

---

7. What are the two ways your users can get the update?

---

---

8. Based on your CSIRT policies, how will you communicate about this incident to your users?

---

---

9. What other useful information did you learn along the way that you can share?

---

---

## Scenario 2 Question Review

1. What are some advisories of interest, articles, and blog posts that may be used as primary sources of information?
2. If your organization runs Windows 8 and Internet Explorer 10, should you be concerned?

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

### Scenario 2 Question Review

Now let's review the answers to your questions.

1. What are some advisories of interest, articles, and blog posts that may be used as primary sources of information?
2. If your organization runs Windows 8 and IE 10, should you be concerned?

## Scenario 2 Question Review

3. According to NIST, what is the CVSS score (out of 10+10+10 or 30)? Does that make you more concerned or less?
4. According to the Adobe Security Bulletin, what are the adverse effects of this malware?

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

### Scenario 2 Question Review

3. According to NIST, what is the CVSS score (out of 10+10+10 or 30)? Does that make you more concerned or less?
4. According to the Adobe Security Bulletin, what are the adverse effects of this malware?

## Scenario 2 Question Review

5. Which release or releases are the vulnerable ones?
6. What are some ways to detect whether a computer has been infected by this vulnerability?

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

### Scenario 2 Question Review

5. Which release or releases are the vulnerable ones?
6. What are some ways to detect whether a computer has been infected by this vulnerability?

## Scenario 2 Question Review

7. What are the two ways your users can get the update?
8. Based on your CSIRT policies, how will you communicate about this incident to your users?

Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

### Scenario 2 Question Review

7. What are the two ways your users can get the update?
8. Based on your CSIRT policies, how will you communicate about this incident to your users?

## **Scenario 2 Question Review**

9. What other useful information did you learn along the way that you can share?

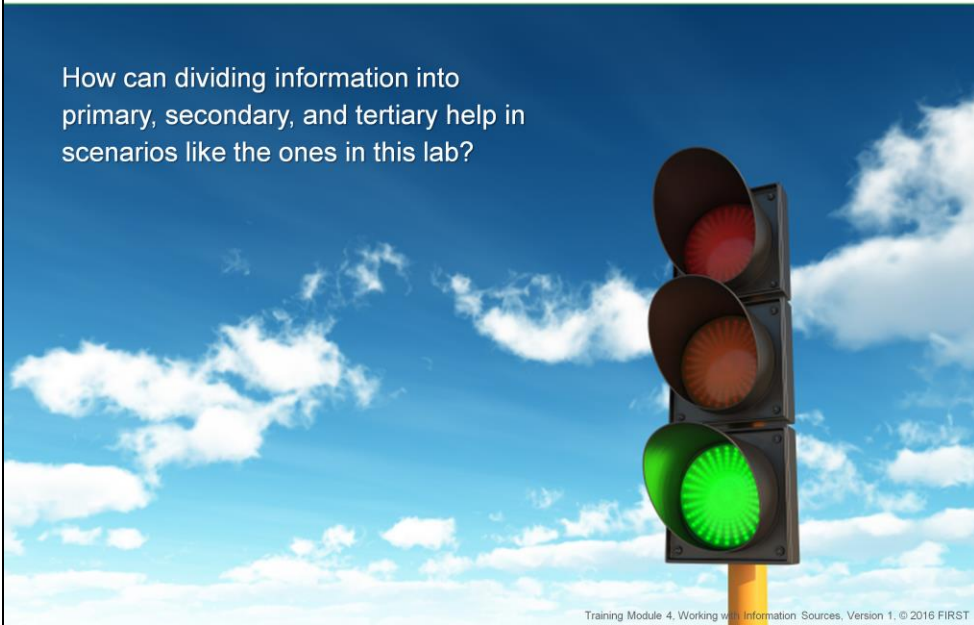
Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST

## **Scenario 2 Question Review**

9. What other useful information did you learn along the way that you can share?

## Learning Check

How can dividing information into primary, secondary, and tertiary help in scenarios like the ones in this lab?



### Learning Check

Now that we've stepped through two scenarios, how can dividing information into primary, secondary, and tertiary help in scenarios like the ones you've experienced in this lab? How will using this methodology help you when responding to an actual incident?



Training Module 4, Working with Information Sources, Version 1, © 2016 FIRST