<CHN>CHAPTER ONE

<CHT>INTRODUCTION TO SECURITY

<COOT>Labs included in this chapter

* <COOH1>Lab 1.1 Online Research—Certification
* Lab 1.2 Online Research—Information Security Careers
* Lab 1.3 Online Research—Threat Actors Ransomware
* Lab 1.4 Online Research—Comparison of Security Breaches and Vulnerabilities
* Lab 1.5 Online Research—Information Security Policies

<COOBT>CompTIA Security+ Exam Objectives

<COOBL>Domain Lab

<COOB>Risk Management 1.3

Technologies and Tools 1.4

Network Security 1.5

<COOB\_LAST>Architecture and Design 1.5

# <H1>Lab 1.1 Online Research—Certification

<H2>Objectives

<TX1>Before starting a new career or changing careers, it’s a good idea to research the field you intend to enter. You may have done so before taking this course; if not, this is the perfect time to begin to research information security certification.

After completing this lab, you will be able to:

* Describe the framework and objectives of the CompTIA Security+ certification exam
* Identify key components of the CompTIA Security+ certification exam

<H2>Materials Required

<TX1>This lab requires the following:

* <BL>A computer with Internet access

<H2>Activity

<FE1TX1>Estimated completion time: **15 minutes**

<TX1>In this lab, you will search the Internet for information on the CompTIA Security+ certification exam objectives.

1. <NL\_FIRST>Open your web browser and go to www.comptia.org.

<B1TX1>It’s not unusual for websites to change the location where files are stored. If the preceding URL no longer functions, use a search engine such as Google to search for “CompTIA Security+ Objectives.”

1. **<NL\_MID>**Click the GO TO CERTIFICATIONS SITE link.
2. Point to the **TRAINING** link at the top of the page,and click the Exam Objectives link.
3. Enter your name, email address, and country in the CompTIA Exam Objectives page.
4. Select the CompTIA Security+ checkbox.
5. Click the SUBMIT button.
6. Click the CompTIA Security+ SY0-401 objectives link for the language of your choice.
7. Review the Security+ Objectivesdocument.
8. Close all windows.

<H2>Review Questions

1. <TF>The smallest percentage of the exam is devoted to Risk Management. True or <TFA>**False</TFA>**?
2. <MULT>Implementing secure protocols is covered under which domain?
   1. <MULTA>Risk Management
   2. **Technologies and Tools**
   3. Identity and Access Management
   4. Threats, Attacks, and Vulnerabilities
3. <MULT>Which of the following is an application/service attack?
   1. **<MULTA>Buffer overflow**
   2. Vishing
   3. Pie thrust
   4. Header manipulation
4. <MULT>Which of the following pieces of hardware is concerned with port security?
   1. <MULTA>Routers
   2. USB ports
   3. **Switches**
   4. Cables
5. <MULT>Which of the following is *not* a software that can be used to assess the security posture of an organization?
   1. <MULTA>Command line tools
   2. Honeypot
   3. Protocol analyzer
   4. **Sniffer**

# <H1>Lab 1.2 Online Research—Information Security Careers

<H2>Objectives

<TX1>The information security field is in its infancy. Its development has lagged behind the development of technology in general. This is evidenced by the relative lack of specific information available on information security job titles and job duties. In this lab, you’ll explore the web for this information and examine an alternative method of determining qualities required for employment in the information security field.

<TX2>After completing this lab, you will be able to:

* <BL>Explain the information security responsibilities of various information technology positions
* Discuss the degree of specificity commonly found in descriptions of information security jobs
* Explain the requirements for information security jobs based on career level, experience, and education

<H2>Materials Required

<TX1>This lab requires the following:

* <BL>A computer with Internet access

<H2>Activity

<FE1TX1>Estimated completion time: **40 minutes**

<TX1>In this lab, you will search the Internet for information on information security careers.

1. <NL\_FIRST>Navigate to www.bls.gov/ooh/.
2. <NL\_MID>This is the Occupational Outlook Handbook, published by the U.S. Department of Labor. In the Search Handbook box on the right side of the page, type information security and click Go.
3. View the first page of results and note how closely the titles relate to information security.
4. Click the links to the first two results.
5. Use your browser’s find on this command to look for information on the security responsibilities of a particular job title.

<NOLB><NO>To access the find on this page command in Windows, use the CTRL+F key combination. On a Mac, use the Command+F combination. </NO>

1. Using your favorite web search engine, spend about 10 minutes finding out what information security workers do by using search strings such as “information security career,” “information security job title,”,and “information security job description.” What is the quality and amount of detail generally available?
2. Navigate to www.wseas.us/e-library/conferences/2009/prague/MCBE/MCBE50.pdf. Read the article “Information Security Employment: An Empirical Study.”

<H2>Review Questions

1. <MULT>In the article “Information Security Employment: An Empirical Study,” the authors found that in the advertised information security jobs, entry-level workers were most commonly required to have \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (Choose all that apply.)
   1. <MULTA>less than one year of experience.
   2. completed high school.
   3. **some college credits.**
   4. one to two years of experience.
2. <MULT>In the article “Information Security Employment: An Empirical Study,” the authors found that in the advertised information security jobs, manager-level workers were most commonly required to have \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (Choose all that apply.)
3. **<MULTA>a bachelor of science or bachelor of arts degree.**
4. seven to ten years of experience.
5. **five to seven years of experience.**
6. some college credits.
7. <MULT>In the article “Information Security Employment: An Empirical Study,” the authors found that \_\_\_\_\_\_\_\_ of security architect positions require a Bachelor’s degree.
   1. <MULTA>50%
   2. 60%
   3. 70%
   4. **85%**
8. <TF>Many information technology job descriptions include some aspect of information security. <TFA>**True** or False?
9. <MULT>In the article “Information Security Employment: An Empirical Study,” the authors found that the most commonly held mid- to high-level information security certification was \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
10. <MULTA>Security+.
11. CISM.
12. **CISSP.**
13. none of the above

# <H1>Lab 1.3 Online Research—Threat Actors Ransomware

<H2>Objectives

<TX1>Threat actors are malicious entities that are responsible for security incidents. In most scenarios, the actor falls into three categories, internal, external, or partnered. Threat actors can come in all forms, but a new favorite mode of attack is to use Ransomware to lock computers and demand users pay a ransom to get their information back.

<TX2>After completing this lab, you will be able to:

* <BL>Define what threat actor is
* Identify the characteristics of Ransomware
* Identify steps to mitigate Ransomware

<H2>Materials Required

<TX1>This lab requires the following:

* <BL>A computer with Internet access

<H2>Activity

<FE1TX1>Estimated completion time: **40 minutes**

<TX1>In this lab, you will search the Internet for information related to organizational security.

1. <NL\_FIRST>Open your web browser and go to **http://www.darkreading.com/threat-intelligence/threat-actors-bring-ransomware-to-industrial-sector-with-new-version-of-killdisk/d/d-id/1327805**.
2. <NL\_MID>Read the article and create a list of different types of Ransomware and their characteristics.
3. Open your web browser and go to **http://www.usatoday.com/story/money/columnist/2016/05/07/ransomware-bad-news-s-getting-worse/83876342/**.
4. Read the article and expand your list of different types of Ransomware and their characteristics.
5. Use the list to form a risk mitigation plan to stop the infection of Ransomware in a company you may or may not work for.
6. Use the risk mitigation plan to create a 2-to-3-page security brief that you would give to your supervisor explaining the risks of Ransomware.

<H2>Certification Objectives

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>1.1 Given a scenario, analyze indicators of compromise and determine the type of malware.
* 5.3 Explain risk management processes and concepts.

<H2>Review Questions

1. <MULT>Which of the following is not a form of Ransomware?
   1. <MULTA>KillDisk
   2. Cryptolocker
   3. CryptXXX
   4. **Bitcoin**
2. <TF>Paying the ransom will always get your information back. True or <TFA>**False</TFA>**?
3. <MULT>Which platform does not have to worry about Ransomware?
   1. <MULTA>Laptops computers
   2. Desktop personal computers
   3. Smartphones
   4. **Smart watches**
4. <MULT>What encryption algorithm is used in the KillDisk Ransomware attacks?
   1. **<MULTA>AES and RSA 1028**
   2. AES and RSA 256
   3. PKI and AES
   4. AES and RSA 512

# <H1>Lab 1.4 Online Research— Comparison of Security Breaches and Vulnerabilities

<H2>Objectives

<TX1>Security is a 24/7 job, requiring a network administrator to seek answers to countless questions. Two particular areas of concern are the overall safety of a network’s operating system and software applications, and managing patches and security solutions. Some questions network administrator might need to answer include: Who makes the safest operating system? What are the known vulnerabilities of each operating system? How many software packages offer patches that people don’t install? In this lab, you’ll explore some of the information available on operating system vulnerabilities.

<TX2>After completing this lab, you will be able to:

* <BL>Research software vulnerabilities
* Analyze vulnerability differences among operating systems

<H2>Materials Required

<TX1>This lab requires the following:

* <BL>A computer with Internet access

<H2>Activity

<FE1TX1>Estimated completion time: **45 minutes**

<TX1>In this lab, you will search the Internet for information on the relative security of several operating systems.

1. <NL\_FIRST>Open your web browser and go to https://www.flexerasoftware.com/enterprise/resources/research/vulnerability-review/tab/browser-security to access the latest Flexera Software Vulnerability Review.
2. <NL\_MID>Click the **Download Now** button.
3. In the Register Now pane, enter the requested information, including your work email, your name, and so on.
4. Click the Read the Report button.
5. Click the **Download Report** button.
6. Navigate to the Vendor Update – Top 50 Portfolio heading. Note the Top 50 vendors who represented 22.5% of the vulnerabilities in 2016.
7. Go to Time-to-Patch on page 17 and note that 81% of vulnerabilities had a patch available on the day of disclosure.
8. Go to Browser Security on page 20. In the first paragraph, it details the percentage of Internet browsers with vulnerabilities and the percentage of products with exploits. Note that there was an increase of 4% of vulnerabilities from 2014 to 2015.
9. Go to http://www.securityfocus.com/archive/.
10. Click the **Complete Archives** linkunder the Bugtraq area. How many links to vulnerability reports do you see? On average, how many vulnerability reports are posted per day on Bugtraq?
11. Browse through the reported issues until you find an operating system vulnerability report. This will give you an idea of the number of application vulnerabilities compared to the number of operating system vulnerabilities.

<H2>Certification Objectives

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.4 Given a scenario, analyze and interpret output from security technologies.

<H2>Review Questions

1. <MULT>According to the Flexera report, the number of zero-day vulnerabilities found in 2016 is \_\_\_\_\_\_\_\_\_\_\_ 2015?
   1. <MULTA>equal to
   2. **less than**
   3. greater than
   4. undetermined
2. <TF>A Vulnerability is equivalent to an exploit. True or <TFA>**False</TFA>**?
3. <MULT>According to the Flexera report, what percentage were without patches for longer than the first day?
   1. <MULTA>13.1%
   2. 22.4%
   3. 5.6%
   4. **19%**
4. <MULT>According to the Flexera report, how many vulnerabilities did Windows 10 have when it was released?
   1. <MULTA>0
   2. **257**
   3. 128
   4. 201
5. <MULT>The purpose of the Bugtraq forum is \_\_\_\_\_\_\_\_\_\_\_?
   1. **<MULTA>to have a location where know issues in software can be saved and stored.**
   2. to give a location where people can exploit operating systems.
   3. to make people afraid of using software.
   4. to help fix vulnerabilities in software.

# <H1>Lab 1.5 Online Research—Information Security Policies

<H2>Objectives

<TX1>Information Security Policies are often instituted as an afterthought to other policies. Acceptable Use Policies and Computer Use Policies are created by organizations to handle individual actions and detail how devices should be used and handled. In this lab, you research various Information Security Policies.

<TX2>After completing this lab, you will be able to:

* <BL>Define the fundamental structure of an Information Security Policy
* Determine the best type of policy for a given situation

<H2>Materials Required

<TX1>This lab requires the following:

* <BL>A computer with Internet access

<H2>Activity

<FE1TX1>Estimated completion time: **40 minutes**

1. <NL\_FIRST>Open your web browser and go to http://www.sans.org/security-resources/policies/.
2. <NL\_MID>Browse through the templates offered and identify key components of the templates.
3. Open a new web browser window and go to your institution’s URL.
4. Search your institution for its Information Security Policy (ISP); it may also be called a Computer Security Policy. Do not mistake this for an Acceptable Use Policy or a Computer Use Policy. You want the document that handles all information security.
5. If you find an ISP, review the document’s structure. Compare the policy with the templates you found on the SANS website. Does the ISP contain sections that are included in other policies? Do these policies match the templates found on the SANS website?
6. If you did not find your institution’s ISP, find either its Computer Use Policy or Acceptable Use Policy. Compare the policy to the templates on the SANS website. Are there similarities? Are there differences?

<H2>Certification Objectives

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.3 Given a scenario, troubleshoot common security issues.
* 4.4 Given a scenario, differentiate common account management practices.
* 5.1 Explain the importance of polices, plans, and procedures related to organizational security

<H2>Review Questions

1. <MULT>This policy defines the acceptable use of equipment and computing services:
   1. <MULTA>Computer Use Policy
   2. **Acceptable Use Policy**
   3. Email Policy
   4. Disaster Recovery Policy
2. <MULT>This policy defines the guidelines and expectations of individuals within the company to demonstrate fair business practices:
   1. <MULTA>Computer Use Policy
   2. Acceptable Use Policy
   3. **Ethics Policy**
   4. Email Policy
3. <TF>A policy is typically a document that outlines specific requirements or rules that must be met. <TFA>**True</TFA>** or False?
4. <MULT>\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ are typically a collection of system-specific procedural requirements that must be met by everyone.
   1. **<MULTA>Policies**
   2. Guideline(s)
   3. Template
   4. Standard
5. <TF>A Computer Security Policy contains other policies that address specific areas of computer infrastructure. <TFA>**True</TFA>** or False?