**Ciampa, *Security+ Guide to Networking Fundamentals*, 6th ed.**

**9781337288781**

**Solutions for Review Questions**

Chapter 1

1. Ian recently earned his security certification and has been offered a promotion to a position that requires him to analyze and design security solutions as well as identifying users’ needs. Which of these generally recognized security positions has Ian been offered?
2. **Security administrator**
3. Security technician
4. Security officer
5. Security manager
6. Alyona has been asked by her supervisor to give a presentation regarding reasons why security attacks continue to be successful. She has decided to focus on the issue of widespread vulnerabilities. Which of the following would Alyona NOT include in her presentation?
7. Large number of vulnerabilities
8. End-of-life systems
9. Lack of vendor support
10. **Misconfigurations**
11. Tatyana is discussing with her supervisor potential reasons why a recent attack was successful against one of their systems. Which of the following configuration issues would NOT covered?
12. Default configurations
13. Weak configurations
14. **Vulnerable business processes**
15. Misconfigurations
16. What is a race condition?
17. When a vulnerability is discovered and there is a raceto see if it can be patched before it is exploited by attackers.
18. **When two concurrent threads of execution access a shared resource simultaneously, resulting in unintended consequences.**
19. When an attack finishes its operation before antivirus can complete its work.
20. When a software update is distributed prior to a vulnerability being discovered.
21. Which the following is NOT a reason why it is difficult to defend against today’s attackers?
22. Delays in security updating
23. **Greater sophistication of defense tools**
24. Increased speed of attacks
25. Simplicity of attack tools
26. Which of the following is NOT true regarding security?
27. Security is a goal.
28. Security includes the necessary steps to protect from harm.
29. Security is a process.
30. **Security is a war that must be won at all costs.**
31. Adone is attempting to explain to his friend the relationship between security and convenience. Which of the following statements would he use?
32. “Security and convenience are not related.”
33. “Convenience always outweighs security.”
34. **“Security and convenience are inversely proportional.”**
35. “Whenever security and convenience intersect, security always wins.”
36. Which of the following ensures that only authorized parties can view protected information?
37. Authorization
38. **Confidentiality**
39. Availability
40. Integrity
41. Which of the following is NOT a successive layer in which information security is achieved?
42. Products
43. People
44. Procedures
45. **Purposes**
46. Complete this definition of information security: *That which protects the integrity, confidentiality, and availability of information* \_\_\_\_\_.
47. *on electronic digital devices and limited analog devices that can connect via the Internet or through a local area network.*
48. *through a long-term process that results in ultimate security.*
49. *using both open-sourced as well as supplier-sourced hardware and software that interacts appropriately with limited resources.*
50. ***through products, people, and procedures on the devices that store, manipulate, and transmit the information.***
51. Which of the following is an enterprise critical asset?
52. System software
53. **Information**
54. Outsourced computing services
55. Servers, routers, and power supplies
56. Gunnar is creating a document that explains risk response techniques. Which of the following would he NOT list and explain in his document?
57. **Extinguish risk**
58. Transfer risk
59. Mitigate risk
60. Avoid risk
61. Which act requires banks and financial institutions to alert their customers of their policies in disclosing customer information?
62. Sarbanes-Oxley Act (Sarbox)
63. Financial and Personal Services Disclosure Act
64. Health Insurance Portability and Accountability Act (HIPAA)
65. **Gramm-Leach-Bliley Act (GLBA)**
66. Why do cyberterrorists target power plants, air traffic control centers, and water systems?
67. These targets are government-regulated and any successful attack would be considered a major victory.
68. These targets have notoriously weak security and are easy to penetrate.
69. **They can cause significant disruption by destroying only a few targets.**
70. The targets are privately owned and cannot afford high levels of security.
71. Which tool is most commonly associated with nation state threat actors?
72. Closed-Source Resistant and Recurrent Malware (CSRRM)
73. **Advanced Persistent Threat** **(APT)**
74. Unlimited Harvest and Secure Attack (UHSA)
75. Network Spider and Worm Threat (NSAWT)
76. An organization that practices purchasing products from different vendors is demonstrating which security principle?
77. Obscurity
78. **Diversity**
79. Limiting
80. Layering
81. What is an objective of state-sponsored attackers?
82. To right a perceived wrong
83. To amass fortune over of fame
84. **To spy on citizens**
85. To sell vulnerabilities to the highest bidder
86. Signe wants to improve the security of the small business where she serves as a security manager. She determines that the business needs to do a better job of not revealing the type of computer, operating system, software, and network connections they use. What security principle does Signe want to use?
87. **Obscurity**
88. Layering
89. Diversity
90. Limiting
91. What are industry-standard frameworks and reference architectures that are required by external agencies known as?
92. Compulsory
93. Mandatory
94. Required
95. **Regulatory**
96. What is the category of threat actors that sell their knowledge of vulnerabilities to other attackers or governments?
97. Cyberterrorists
98. Competitors
99. **Brokers**
100. Resource managers

# **Chapter 1**

**Introduction to Security**

|  |
| --- |
| **At a Glance** |

#### Instructor’s Manual Table of Contents

* Overview
* Objectives
* Teaching Tips
* Quick Quizzes
* Class Discussion Topics
* Additional Projects
* Additional Resources
* Key Terms

|  |
| --- |
| Lecture Notes |

# **Overview**

Chapter 1 introduces security fundamentals that form the basis of the Security+ certification. It begins by examining the current challenges in computer security and why it is so difficult to achieve. It then describes information security in more detail to illustrate why it is important. Finally, the chapter looks at who is responsible for these attacks and what the fundamental defenses against attackers are.

# **Chapter Objectives**

* Explain the challenges of securing information
* Define information security and explain why it is important
* Identify the types of threat actors that are common today
* Describe how to defend against attacks

# **Teaching Tips**

**Challenges of Securing Information**

1. Explain that there is no simple solution to securing information. This can be seen through the different types of attacks that users face today, as well as the difficulties in defending against these attacks.

**Today’s Security Attacks**

1. Describe some recent security attacks, such as the following:
   1. A reporter drove a Jeep Cherokee while two security researchers 10 miles away remotely connected to it and started manipulating its controls.
   2. United Airlines passenger who tampered with the Seat Electronic Box to connect to other system on the plane.
   3. Half a billion Yahoo accounts were compromised by attacker who gained unauthorized access to its web servers.
   4. USB Killer device.
   5. WINVote voting machine vulnerabilities .
   6. VTech accounts that included information on 6.4 million children were hacked .
   7. IRS Get Transcript program was hacked.
2. Mention that security statistics bear witness to the continual success of attackers:
   1. From 2005-2017 over 907 million electronic data records in the U.S. had been breached.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Phishing Web sites are well known for suddenly appearing and then disappearing to reduce the risk of being traced. The average time a site is online is only four days according to the APWG ([www.antiphishing.org](http://www.antiphishing.org)). |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | The US-CERT security bulletin is available at [www.us-cert.gov/cas/bulletins/](http://www.us-cert.gov/cas/bulletins/). |

**Reasons for Successful Attacks**

1. Discuss the following reasons behind successful attacks:
   1. Widespread vulnerabilities
   2. Configuration issues
   3. Poorly designed software
   4. Hardware limitations
   5. Enterprise-based issues

**Difficulties in Defending against Attacks**

1. Describe the following difficulties in defending against attacks:
   1. Universally connected devices
   2. Increased speed of attacks
   3. Greater sophistication of attacks
   4. Availability and simplicity of attack tools
   5. Faster detection of vulnerabilities
   6. Delays in security updating
   7. Weak security update distribution
   8. Distributed attacks
   9. Use of personal devices
   10. User confusion
2. Table 1-2 summarizes these difficulties.

**What Is Information Security?**

1. Mention that knowing why information security is important today and who the attackers are is beneficial. Point out that knowing the terminology used can be helpful when creating defenses for computers.

**Understanding Security**

1. Explain that security can be considered as a state of freedom from a danger or risk. This state or condition of freedom exists because protective measures are established and maintained.
2. Use Figure 1-2 to help explain the relationship between security and convenience. Point out that as security is increased, convenience is often decreased.

**Defining Information Security**

1. Define information security as the tasks of guarding information that is in a digital format. It ensures that protective measures are properly implemented. Information security cannot completely prevent attacks or guarantee that a system is totally secure.
2. Explain that information security is intended to protect information that has value to people and organizations. That value comes from the characteristics of the information:
   1. Confidentiality
   2. Integrity
   3. Availability

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | The confidentiality, integrity, and availability of information is known as CIA. |

1. Explain that information security is achieved through a combination of three protections. Use Figure 1-3 and Table 1-3 to illustrate your explanation.
2. Emphasize that information security is that which protects the integrity, confidentiality, and availability of information on the devices that store, manipulate, and transmit the information through products, people, and procedures.

**Information Security Terminology**

1. Define the following information security terms:
   1. Asset
   2. Threat
   3. Threat actor
   4. Vulnerability
   5. Attack vector
   6. Attack surface
   7. Risk
2. Use Figure 1-4 and Table 1-5 to illustrate the terminology above.
3. Discuss and define the different options available when dealing with risks.
4. Acceptance
5. Transference
6. Risk avoidance
7. Mitigation

**Quick Quiz 1**

1. Which protection ensures that only authorized parties can view the information?
2. Confidentiality
3. Integrity
4. Accounting
5. Availability

Answer: A

1. Which of the following terms best describes ensuring that data is accessible to authorized users?
   * 1. Integrity
     2. Accounting
     3. Availability
     4. BYOD

Answer: C

1. A(n) \_\_\_\_ is defined as something that has a value.

Answer: asset

1. A situation that involves exposure to some type of danger is known as which of the following?
2. vector
3. risk
4. threat
5. asset

Answer: B

1. Addressing a risk by making it less serious is known as which of the following?
2. acceptance
3. transference
4. avoidance
5. mitigation

Answer: D

**Understanding the Importance of Information Security**

1. Mention that the main goals of information security are to prevent data theft, thwart identity theft, avoid the legal consequences of not securing information, maintain productivity, and foil cyberterrorism.
2. Explain that security is often associated with theft prevention. The theft of data is one of the largest causes of financial loss due to an attack. Individuals are often victims of data thievery.
3. Mention that identity theft involves using someone’s personal information to establish bank or credit card accounts that are then left unpaid, leaving the victim with the debts and ruining their credit rating.
4. Explain that a number of federal and state laws have been enacted to protect the privacy of electronic data, including the following:
   1. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
   2. The Sarbanes-Oxley Act of 2002 (Sarbox)
   3. The Gramm-Leach-Bliley Act (GLBA)
   4. Payment Card Industry Data Security Standard (PCI DSS)
   5. State notification and security laws

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | In 2008, California extended its data breach notification law to encompass incidents including electronic medical and health insurance information. |

1. Explain that cleaning up after an attack diverts resources such as time and money away from normal activities. Use Table 1-6 to illustrate your explanation.
2. Define cyberterrorism as attacks by terrorist groups using computer technology and the Internet. Utility, telecommunications, and financial services companies are considered prime targets of cyberterrorists.

**Who Are the Threat Actors?**

1. Explain that the term threat actor, in a generic sense, is used to describe individuals who launch attacks against other users and their computers.
2. Explain that threat actors of today have a more focused goal of financial gain: to exploit vulnerabilities that can generate income.
3. Point out that the characteristic features of different groups of threat actors can vary widely:
   1. Sophisticated
   2. Funding and resources
   3. External or internal to the enterprise
   4. Intent and motivation
4. Today threat actors are recognized in more distinct categories, such as script kiddies, hactivists, nation state actors, insiders, and others.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Security vulnerabilities, however, can be exposed in ways other than attacking another computer without the owner’s consent, and most security professionals would not refer to themselves as hackers. |

**Script Kiddies**

1. Define script kiddies as individuals that want to break into computers to create damage. They download automated hacking software (scripts) from Web sites and use it to break into computers.
2. Point out that script kiddies can acquire entire exploit kits from other attackers. It takes little skill to be a script kiddie.

#### Hactivists

1. Mention that hactivists are a group strongly motivated by ideology. They are likely to break into a website and change the contents as a means of making a political statement.
2. Point out that it is estimated that there are thousands of hacktivist groups worldwide supporting a wide variety of causes.

#### Nation State Actors

1. Define nation state actors as individuals hired by governments to launch computer attacks against the country’s foes.
2. Mention that a new class of attacks called Advanced Persistent Threat (APT) have been created. Further explain that these attacks uses innovative attack tools and once a system is infected it silently extracts data over an extended period.

**Insiders**

1. Mention that one of the largest information security threats to a business actually comes from an unlikely source: its employees, contractors and business partners.
2. Describe some of the reasons an employee would break into their company’s computer, including:
   1. Disgruntled employees may be intent on retaliating against the company
   2. Industrial espionage
   3. Blackmailing

**Other Threat Actors**

1. Use Table 1-7 to discuss the characteristics of the different types of attackers mentioned in this section of the text.

**Defending Against Attacks**

1. Mention that although multiple defenses may be necessary to withstand an attack, these defenses should be based on five fundamental security principles: layering, limiting, diversity, obscurity, and simplicity.

**Layering**

1. Mention that information security must be created in layers.
2. Explain that one defense mechanism may be relatively easy for an attacker to circumvent. Instead, a security system must have layers, making it unlikely that an attacker has the tools and skills to break through all the layers of defenses.
3. Explain that a layered approach (also called defense-in-depth) can also be useful in resisting a variety of attacks. Layered security provides the most comprehensive protection.

**Limiting**

1. Mention that limiting access to information reduces the threat against it.
2. Explain that only those who must use data should have access to it. In addition, the amount of access granted to someone should be limited to what that person needs to know.
3. Mention that some ways to limit access are technology-based, while others are procedural.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | What level of access should users have? The best answer is the least amount necessary to do their jobs, and no more. |

**Diversity**

1. Explain that layers must be different (diverse) so that if attackers penetrate one layer, they cannot use the same techniques to break through all other layers.
2. Using diverse layers of defense means that breaching one security layer does not compromise the whole system.

**Obscurity**

1. Explain that an example of obscurity is not revealing the type of computer, operating system, software, and network connection that a computer uses. An attacker who knows that information can more easily determine the weaknesses of the system.
2. Mention that obscuring information can be an important way to protect information.

**Simplicity**

1. Explain that information security is by its very nature complex. Complex security systems can be hard to understand, troubleshoot, and feel secure about.
2. Mention that as much as possible, a secure system should be simple for those on the inside to understand and use. Complex security schemes are often compromised to make them easier for trusted users to work with. Keeping a system simple from the inside but complex on the outside can sometimes be difficult but reaps a major benefit.

**Frameworks and Reference Architectures**

1. Explain that industry-standard frameworks and reference architectures provide a resource of how to create a secure IT environment.
2. Point out to students that various frameworks/architectures are specific to a particular sector (industry-specific frameworks) such as the financial industry.
3. Discuss how some of the framework/architectures are domestic while others are worldwide (national vs. international).

**Quick Quiz 2**

1. \_\_\_\_\_\_\_ is a generic term used to describe individuals who launch attacks against other users and their computers.

Answer: Threat actors

1. The motivation of which type of threat actor may be defined as ideology, or attacking for the sake of their principles or beliefs?
2. script kiddies
3. hactivists
4. nation state actors
5. insiders

Answer: B

1. Attackers who do their work by downloading automated attack software from websites and use it to perform malicious acts are known as which of the following?
2. script kiddies
3. hactivists
4. nation state actors
5. insiders
6. Answer: A
7. In which fundamental security principle would only those personnel who must use data have access to it?
8. layering
9. limiting
10. diversity
11. obscurity

Answer: B

1. Which fundamental security principle involves not revealing the type of computer, version of operating system, or brand of software that is used?
2. layering
3. limiting
4. diversity
5. obscurity

Answer: D

# **Class Discussion Topics**

1. What are the differences between hactivists and state-sponsored attackers?
2. Ask students to explain why creating a defense-in-depth is a good strategy when creating a secure IT environment.

# **Additional Projects**

1. Ask your students to read more about phishing scams and write a report with a series of guidelines to recognize them and other fraudulent e-mails.

Nessus is a widely used free vulnerability scanner tool used by many security experts. Ask your students to read more about Nessus and write a report summarizing its more important features.

# **Additional Resources**

1. FTC – Computer Security

<http://www.consumer.ftc.gov/topics/computer-security>

1. Fight Spam on the Internet!

<http://spam.abuse.net/>

1. How to recognize phishing e-mail messages, links, or phone calls

<http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx>

1. Anti-Phishing Working Group

<http://www.antiphishing.org/>

1. SANS' Information Security Reading Room

<http://www.sans.org/reading_room/>

1. Zero day initiative

<http://www.zerodayinitiative.com/>

**Key Terms**

* **accept**
* **administrative controls**
* **Advanced Persistent**
* **Threat (APT)**
* **architecture/design**
* **weaknesses**
* **asset**
* **attributes**
* **availability**
* **avoid**
* **competitors**
* **confidentiality**
* **control diversity**
* **default configurations**
* **defense-in-depth**
* **end-of-life system**
* **external**
* **funding and resources**
* **hactivists**
* **improper error**
* **handling**
* **improper input handling**
* **improperly configured**
* **accounts**
* **industry-specific**
* **frameworks**
* **industry-standard**
* **frameworks**
* **insiders**
* **integrity**
* **intent and motivation**
* **internal**
* **international**
* **lack of vendor support**
* **layered security**
* **misconfiguration**
* **mitigate**
* **nation state actors**
* **national**
* **new threat**
* **non-regulatory**
* **open-source intelligence**
* **organized crime**
* **race condition**
* **reference architectures**
* **regulatory**
* **resource exhaustion**
* **risk**
* **risk response**
* **techniques**
* **script kiddies**
* **sophisticated**
* **system sprawl**
* **technical controls**
* **threat**
* **threat actor**
* **transfer**
* **undocumented assets**
* **untrained users**
* **user training**
* **vendor diversity**
* **vulnerability**
* **vulnerable business**
* **processes**
* **weak configuration**
* **zero day**

<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?

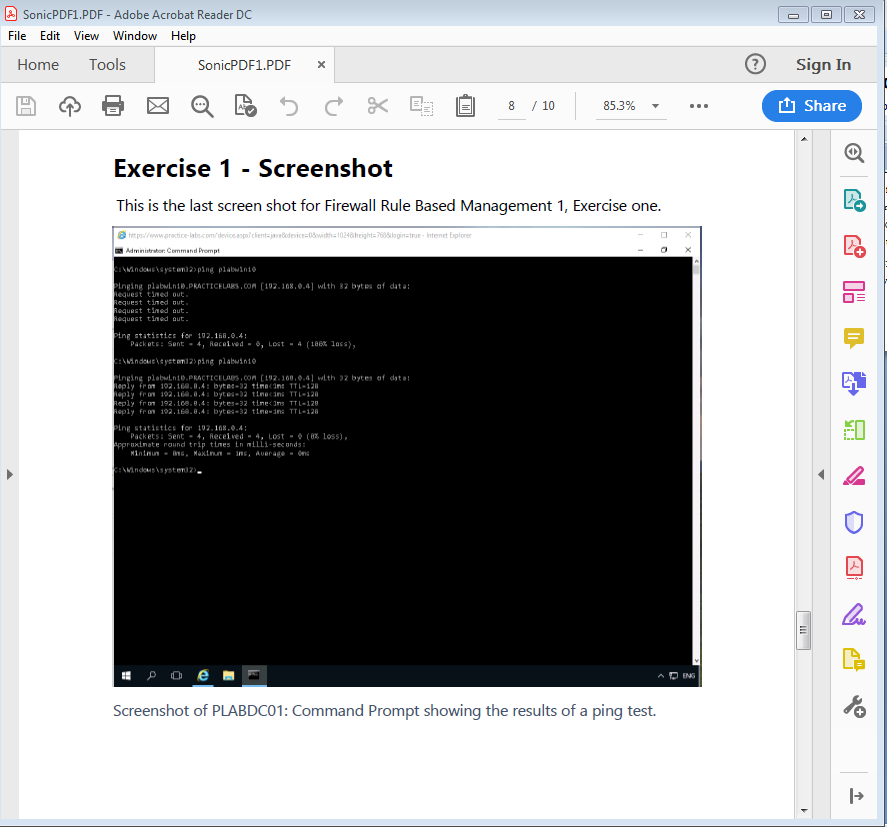
<H2>Certification Objectives

<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?

****