CompTIA Security+ Study Guide (SY0-501)

Labs

As you will find, the Security+ curriculum is not a very "hands-on" curriculum. Therefore, most of these labs are discussion and are designed to get the student to think about situations and come up with "best case" answers, based on the criteria given. It is important to remember that many of these discussions are purposely open ended and are designed to get the student to think in terms of "what is the *best* answer" and not "what is the *right* answer."

It is also important to note that the use of these labs is entirely optional. They are designed to reinforce items in the *CompTIA Security+ Study Guide* that you may want to focus on during the course.

Sample Lab 1: Security Basics Discussion

Describe a situation in which you observed a lack of concern for security, preferably in a public place or business and discuss it with your peers. Discuss where they could have made their situation more secure. Spend some time focusing on weaknesses of mobile devices (ranging from laptops to smartphones). Discuss the fact that *any* activity that involves sharing personal identifiable information (PII) via WiFi, hotspots, e-mail, or text messages needs to be protected and discuss ways to check for mobile security apps on iTunes, Google Play, and so on.

Understand the importance of manually locking your phone, laptop, or other devices when not in use. Since they are so easy to steal and then access, never walk away from a device you have logged into without locking it and always configure said devices to lock automatically after a period of inactivity.

Sample Lab 2: Film Homework

Have students watch the old movie *Sneakers* either by themselves or with the class. Then, have them report on which methods of cryptography (and the cracking of it) they noticed in the film and how well the film stands the test of time.

Sample Lab 3: Real-World Scenario Discussion

Discuss the following real-world scenario. What would you do? Discuss the options with your class.

You Be the Judge

You have been monitoring the activities of users in your company. You unintentionally intercepted an e-mail on the system indicating that one of the key employees in the organization has a drug problem and is in a treatment program. What should you do with this information?

This is a tough situation to be in, and one you will find yourself in more often than you want. This information was gained by accident, and it is potentially embarrassing and sensitive in nature. You would probably be best served by not disclosing this information to anyone. If you are uncertain, you should discuss the general situation with your human resource (HR) department. Avoid specifics of this situation until you know how the company wants to handle this situation. There are both ethical and legal issues involved in this situation. You will have to find your way through this situation. However, you should never discuss this situation with anybody without first consulting with an HR representative, and you should certainly never discuss this with anybody but authorized personnel.

Sample Lab 4: Firewalls

Compare the features the firewall methods used by a few different models of corporate firewall. Some common brands include the following:

- Barracuda (from Barracuda)
- SonicWALL (from Dell)

- Cisco ASA, Meraki, and PIX (from Cisco)

Sample Lab 5: Web Demonstration

https://www.symantec.com/security-center

Go to the Security Center website from Symantec and show the resources that are posted there, including recent blog entries. Then click to display the most recent Internet Security Threat Report (which requires you to enter a name). This will give you information on the latest malicious code threats, the details of a particular threat, removal tools, and any other information related to the detection and removal of malicious code.

Sample Lab 6: Download and Install a Free Antivirus Utility

AVG is a free antivirus protection software. While not as full featured as other antivirus programs, it still allows passive and active detection of virus activity, as well as the ability to update virus signatures. And, you can't beat the price.

1. Using a computer with an Internet connection, start the Internet connection and web browser.
2. Go to the website www.avg.com/us-en/homepage and download the free version of AVG using the links on the main page. You may have to fill out a form giving your address and e-mail address. Be sure to read any license agreements. Save the installation program file in your My Documents folder.
3. Once the software is downloaded, navigate to your My Documents folder and double-click the installer program to begin installing the software.
4. Follow the installation prompts, entering the serial number that is sent to your e-mail (at the appropriate time when asked to do so). Also, answer any other questions the installer program asks.
5. Finish the installation of the software and do a scan of your computer for viruses.

Sample Lab 7: Authentication Concepts Discussion

You are the IT staff person tasked with implementing security for your organization, a small manufacturing firm. The company you work for has 50 employees, is headquartered in a small town, and does modest business worldwide. The budget for security is small, but management will go with your recommendation, if budget requirements must be increased. Discuss the merits of the different authentication methods you might use for your organization. Include such points as overall cost to implement, security level, and requirements of the users.

Sample Lab 8: Privilege Management

Using the book and the websites listed, compare and contrast the different methods of single sign-on (SSO) as implemented by Microsoft Active Directory (http://msdn.microsoft.com/en-us/library/aa745042(v=bts.10).aspx).

Sample Lab 9: War Driving

Group students into groups of two or three. Have each group give a five-minute presentation to the rest of the class on the practice of war driving. Have them try to obtain the software from the Internet that would allow a person to go on a war drive to illustrate how easy it is to do. Demonstrations of war driving are not necessary and should be discouraged. A discussion of war chalking, and the symbols used for it, should be included.

Sample Lab 10: Research Computer Ethics

Using the website of Computer Professionals for Social Responsibility (CPSR) at http://cpsr.org/, read about computer ethics and their use in business today ("Technology and Ethics" is located on the Issues tab). Incorporate student findings into class discussion.

Sample Lab 11: Appreciating That the Ability

to Access Does Not Grant an Unlimited Right

It is key for anyone with more than basic user privileges to understand that the legitimate use of resources does not extend to whatever one is capable of doing with them. Although information security controls could permit access, for example, that does not mean a person should access confidential information unless they have a legitimate reason for so doing.

Sample Lab 12: Downloading and Installing a Patch or Fix

Have students download and install an operating system or application patch. Microsoft service packs are the best to illustrate how they are applied. Use the following site for additional help: https://www.microsoft.com/en-us/download.

Sample Lab 13: Web Research and Discussion

Perform a web search using your favorite search engine (Google, Bing, etc.) on some of the most popular methods used to implement various types of attacks. For example, look for the methods used to start a denial-of-service (DoS) attack like which software is used, the motives behind DoS, and so on. Then, discuss with the class about ways to prevent these attacks or at least minimize their effects on your organization.

Sample Lab 14: The Decoder Wheel

To understand encryption, have them make a decoder wheel. Pair up the students. On the chalkboard or whiteboard, draw a ring of alphanumeric characters that includes every letter in the alphabet and the numbers 0 through 9. Inside that ring, draw another ring of the same set of alphanumeric characters but drawn in such a way so that each character on the inner ring matches up with a different character on the outer ring. Students can use the design you draw on the chalkboard or come up with their own. But, each pair should have the exactly the same “wheel.”

Illustrate that the decoder wheel is the key and can be given to the recipient "out of band" either by mail or by personal delivery.

Have one of the people in the pair write a message and encrypt it using the wheel. The inner ring is the standard letter, and the outer ring is the coded letter. Then, have that person send the message on to the recipient in code. The recipient must then decode the message using the same decoder wheel, except that they must then find the letter in code on the outer ring and match it up with the standard letter on the inner ring in order to decode the message.

Finally, if time permits, have other members of the class try to decode the message without the key. If necessary, make up your own key and don't give it to the class. Then, pass out the coded message. The coded message will be extremely difficult to decode, if not impossible. Impress upon the students that such a simple coding mechanism is often still used because of its effectiveness and simplicity. But, with computers, such codes are becoming much easier to crack.

Sample Lab 15: Using OpenPGP

Download OpenPGP and encrypt an e-mail, and then send it to another classmate, who must then try to decrypt it. OpenPGP can be found at www.openpgp.org/.

Sample Lab 16: Key Lifecycle

Make a study aid flowchart that shows the key lifecycle using the topics found in the book, starting from key generation and including key expiration, revocation, and archiving.

Sample Lab 17: Draft an Acceptable Use Policy (AUP)

Working completely from scratch, ask students to draft what they would put into an AUP for users of a new organization that is just starting up and hiring its first employees. Mention that many organizations now break acceptable use into at least three categories that are defined in the employee manuals: permitted personal use, permitted commercial use, and spelled-out uses that are not permitted. For example, personal use of a

company's PC and resources is often allowed provided the usage adheres to all applicable policies *and* does not result in additional costs to the organization. Permitted commercial use typically relates to research and sponsored programs, while spelled-out nonpermitted uses include anything violating legal obligations, anything of private financial gain, political campaigning, accessing pornographic, and so on. The policy must unequivocally state that under no circumstances may incidental personal or commercial usage involve violations of the law, interfere with the fulfillment of an employee's responsibilities, or adversely impact or conflict with activities supporting the mission of the organization.

Sample Lab 18: Security Education

Find and research sources of up-to-date security information, either on the Internet or through periodicals (some of which are listed in the book). Discuss the merits of each that you find with the rest of the class.

Sample Lab 19: Visual Guides to Social Engineering

Have students read the Visual Guide to Disruptive Attacks posted at http://certmag.com/picture-this-a-visual-guide-to-disruptive-attacks/ and the Visual Guide to Hard Copy Sanitation at http://certmag.com/picture-visual-guide-hard-copy-sanitation/. With a partner, discuss procedures that could be implemented to prevent these methods from being successful in your environment.

Sample Lab 20: Physical Security

Discuss with your classmates the different types of physical security that might affect communications security.

Sample Lab 21: Investigate Keyloggers

Go to a search engine and enter **keylogger** as the search criteria. Then examine the results returned. How easy is it to obtain something that would keep a log file of all keystrokes (including passwords) a co-worker

made? How easy would it be to retrieve that data? How could you, as an administrator, prevent this from happening?

Sample Lab 22: Proliferation of Password-Cracking Utilities

Do a search in your favorite Internet search engine on the words *password crack* and notice how many sites there are devoted to this practice. Discuss with your classmates the differences between the different utilities. Notice how some are even endorsed by major trade publications.

Follow up by discussing ways to decrease the likelihood of success these crackers may have on your systems by enforcing strong, complex passwords and multifactor authentication. A strong password policy requires at least 12 characters in length and must include at least three of the four different types of characters (uppercase, lowercase, numbers, symbols). Since it is recommended that users use a different password for different websites and applications, look into how a password management tool can help keep track of passwords across multiple sites.

Sample Lab 23: Business Continuity Evaluation

Using a major disaster as your starting point (9/11, Hurricane Katrina, etc.), research a few of the companies that were working in the zone affected by the disaster and what their business continuity plans were. Then, evaluate their effectiveness (i.e., were they able to continue business after that disaster—why or why not?) and discuss with the other students in the class.

Sample Lab 24: Backup Discussion

Discuss with your classmates your current method(s) of data backup and then critique your own and others from the standpoint of security. Are backups done at all? Are the backups done in a secure fashion? Are the tapes physically secure?

Sample Lab 25: Backup Report

Create a 500 to 1,000-word report on the different methods of backup being used today, including tape, online, near-line, cold-side, and hot-site backups. Include a table that shows the difference between a full backup, a differential backup, and an incremental backup.

Sample Lab 26: Sample Disaster Recovery Plan

Create a sample disaster recovery plan for a company that manufactures pens and other writing utensils. Include contingencies for natural disasters, robbery, death of a key employee, and any others you choose. Also include the ability to recover all data and return to full production within one week using whatever methods necessary. The budget is close to unlimited but should be no more than $1 million. This exercise may take some time, so it should be done as a homework assignment. Use the Internet to research common aspects of a disaster recovery plan.

Sample Lab 27: Packet Sniffing Article

Read the online article on Carnivore, the U.S. government's packet sniffing spy utility at http://computer.howstuffworks.com/carnivore.htm.

If necessary, this article could be printed out in advance and given to the students. Ask students which side of the controversy they agree with. In other words, is it OK for the FBI to read people's e-mail? Ask them, then, what they think of the fact that the program was replaced several years ago with "commercially available" software that others could also obtain.

Sample Lab 28: Guest Speaker on Forensics

Invite a local law enforcement official to speak for 20 minutes on the science of forensics as they apply to law enforcement. If possible, a demonstration of forensic methods (especially those that apply to computer forensics) would be most helpful. The speaker should demonstrate collection and preservation of evidence as well as chain of custody.

Sample Lab 29: Spam

Present an example of an e-mail header that shows the path an e-mail takes from sender to receiver. Double-click the e-mail and then choose File ➢ Properties to show the properties of the e-mail (or Inspect Element or View Page Info). The header can be found on the Details tab in the Properties window.

Sample Lab 30: Another Helping of Spam

Discuss with the class the methods of spammers, including their use of ISPs, bulk-email programs, e-mail harvesting tools, and so on. Move the discussion from spam to other forms of e-mail based attacks such as phishing. PayPal and eBay are common targets for phishing attempts, and you can go to either web site and find useful information about how to identify and respond to phishing expeditions. Know that deceptive links take you to deceptive websites.