<CHN>CHAPTER NINE

<CHT>Client and Application Security

<COOT>Labs included in this chapter

* <COOH1>Lab 9.1 Verifying the Integrity of the Hosts File
* Lab 9.2 Installing the FTP Server Service and Wireshark
* Lab 9.3 Capturing and Analyzing FTP Traffic
* Lab 9.4 Physical Security Planning
* Lab 9.5 Data Loss Prevention

<COOBT>CompTIA Security+ Exam Objectives

<COOBL>Domain Lab

<COOB>Threats, Attacks, and Vulnerabilities 9.3

Techniques and Tools 9.1, 9.2, 9.3, 9.4, 9.5

Risk Management 9.4, 9.5

Architecture and Design 9.2, 9.3, 9.4, 9.5

Cryptography and PKI 9.1

# <H1>Lab 9.1 Verifying the Integrity of the Hosts File

**<H2>Objectives**

<TX1>When computers were first connected by transmission media, there were very few computers to connect. Networking protocol stacks, such as TCP/IP, were just being developed, and only a few computers, mostly at universities, were connected. There was no need for the Domain Name System (DNS), which is the massive, distributed, world wide database of computer addresses that we use now. Early networked computers did need the ability to find each other, and some sort of address directory was needed. The TCP/IP solution was to create a text file that contained the name and address of each computer on the network. This file, called hosts, was copied to all the networked computers. If a new computer was added (which was not a common event), a letter was sent or a phone call was made, letting the computer scientists know the changes they should make to the hosts file.

<TX2>The hosts file is still used today. The file can contain the IP addresses of computers as well as their fully qualified domain names (for example, 172.31.157.33 server01.compcol.net). In fact, most systems have nothing more than the local loopback address listed in the hosts file. We have the DNS system of distributed databases, and the millions of computers on the Internet query these DNS servers to find out a system’s IP address. Note, however, that these DNS queries can take up a lot of network bandwidth. This is why some administrators still use the hosts file. When a client tries to resolve a fully qualified domain name (FQDN), such as server01.compcol.net, to its IP address, such as 172.31.157.33, the first thing the client does is determine if its own FQDN is server01.compcol.net. When this query comes back negative, instead of querying its DNS server right away, the client checks its own hosts file. If server01.compcol.net is a system that an organization’s users access frequently, the network administrator might have entered server01’s resolution information in the hosts files of all workstations in the company so that the network bandwidth isn’t used unnecessarily in querying the DNS server.

However, the hosts file is a vulnerability. If an attacker modified a client’s hosts file so that the attacker’s server address was listed instead of the real IP address, the client would be redirected to the fake server. Obviously, this would be a serious security breach. Thus, it is important for network security personnel to know when the hosts file, or any other important system file, changes without authorization. Intrusion detection techniques usually monitor this kind of activity, and in this lab, you learn the technique used by some IDS systems—a cryptographic technique called hashing—to monitor the validity and integrity of system files.

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

* <BL>Detect changes to a system file using hashing
* Explain the mechanism used by intrusion detection systems to monitor unauthorized changes to system files

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows Server 2016 or Windows 10 VM

**<H2>Activity**

<FE1TX1>Estimated completion time: **15–20 minutes**

<TX1>In this lab, you download a cryptographic hashing tool and test the integrity of your hosts file before and after its modification.

1. <NL\_FIRST>Log on to either Windows 10 VM or Windows Server with an administrative account, open your web browser, and go to <URL>**https://github.com/jessek/hashdeep/releases/tag/release-4.4</URL>.**

[BEGIN NOTE]

<B1TX1>It is not unusual for websites to change where files are stored. If the suggested URL no longer functions, open a search engine such as Google and search for “md5deep”.

[END NOTE]

1. <NL\_MID>Scroll down and click the md5deep-4.4.zip link.
2. Internet Explorer may block the file download and display a message bar on top of the webpage. If so, click this bar and click Download File. On the File Download window, click Save, and in the Save As window, save the file to your desktop.
3. Close the Download complete window and close your web browser.
4. Double-click the md5deep-4.4 archive file on your desktop. In the md5deep window, click Extract. Then click Extract all files, and in the Extract Compressed (Zipped) Folders window, click the Browse button and navigate to Local Disk (C:). Click OK in the Select a destination window, and click Extract.
5. For ease in navigation from the command prompt, rename the md5deep-4.4 folder to md5.
6. Open Notepad. From the File menu, click Open and navigate to C:\Windows\System32\drivers\etc. In the drop-down box that says Text Documents (\*.txt), change the setting to All Files. Open the hosts file. (See Figure 9-1.)

**[Insert Figure 9-1 Here]**

1. Note that the first lines are preceded by the # sign. This symbol tells the operating system to disregard the lines. These lines are remarks for the user to read and are said to have been “rem’ed out” (remarked out). Your hosts should be similar to those shown in Figure 9-1. The last two lines provide the system’s IPv4 and IPv6 loopback addresses, which tell the system how to refer to itself. Note that on Windows 10 VM and Windows Server these last two lines are rem’ed out.
2. Close the hosts file. Click Start, type cmd, and press Enter.
3. At the command prompt, type cd C:\md5 to navigate to the md5 directory and then type dir and press Enter.
4. Notice that several files have an .exe extension. These allow you to hash files using different hashing algorithms.
5. At the command prompt, type sha256deep C:\Windows\System32\Drivers\etc\hosts and press Enter.
6. Highlight and copy the hash to the clipboard (see Figure 9-2).

**[Insert Figure 9-2 Here]**

1. Open Notepad, right-click anywhere inside the blank Notepad document, and select Paste. Your hash of the hosts file should appear. From the File menu, click Save As. In the File name box, type hosthash. In the *Save as type* box, verify that Text Documents (.txt) is selected. Navigate to your desktop, click Save, and then close the file.
2. Open Notepad with Administrative privileges and, if necessary, click Yes in the User Account Control box. From the File menu, click Open, navigate to the hosts file, and open it. Add the following line to the bottom of the file: 69.32.133.79 www.boguswebaddress.net. From the File menu, click Save and then close the hosts file.
3. Repeat Steps 13 and 14, and then open hosthash.txt and paste the second hash in the file. Compare the two hashes. Do the two hashes look similar? If this process were automated for all system files, it would be easy to tell when a file has been altered.
4. Open your web browser and go to <URL>www.boguswebaddress.net</URL>. Explain the results.
5. Close all windows and log off.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.6 Given a scenario, implement secure protocols.
* 6.0 Compare and contrast basic concepts of cryptography.
* 6.2 Explain cryptography algorithms and their basic characteristics.

**<H2>Review Questions**

1. <MULT>What is the DNS record type for an IPv6 address?
   1. <MULTA>A
   2. AA
   3. **AAAA**
   4. AV6
2. <MULT>What is the IPv6 loopback address?
   1. <MULTA>0.0.0.0
   2. 127.0.0.1
   3. 255.255.255.255
   4. **::1**
3. <MULT>How many hexadecimal characters are needed to express 256 bits?
   1. **<MULTA>16**
   2. 32
   3. 64
   4. 128
4. <MULT>Which of the following statements regarding hashes is true?
   1. <MULTA>When a 200 MB file that has been previously hashed has one byte changed, a second hash of the file will be nearly similar to the first hash.
   2. When a 200 MB file that has been previously hashed has one byte changed, a second hash will be more similar to the first if SHA1 were used than if SHA256 were used.
   3. When a 200 MB file that has been previously hashed has one byte changed, a second hash of the file will be much less similar to the first hash than would be the case if the file had only been 200 KB in size.
   4. **When a file of any size is modified, there is no relationship between the pre- and post-modification hashes and the number of bytes modified.**
5. <FIB>Hashing is a useful tool in \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   1. **<FIBA>intrusion detection**
   2. maintaining data availability
   3. prevention of unauthorized file modification
   4. the development of secure cryptographic algorithms

# <H1>Lab 9.2 Installing the FTP Server Service and Wireshark

**<H2>Objectives**

<TX1>The most common way to maintain the confidentiality of data in transit is to use encryption. The assumption is that even if an attacker were to capture (sniff) the traffic, the expense and time required to decrypt the data without the decryption key would be prohibitive. On the other hand, traffic that is not encrypted is readily available to anyone with access to the network medium and a protocol analyzer. With the growing number of wireless networks, it is very easy to get access to the network medium; it is in the air. At a café with wireless Internet access or in the parking lot outside an office building, wireless transmissions may be captured and analyzed by relatively unsophisticated attackers. Many people transmit their logon credentials “in the clear”—that is, unencrypted (usually called plaintext)—without being aware of it. Generally speaking, when you open your email client to check your email, your username and password for your mail server account are transmitted unencrypted. This is true of many DSL connections, too.

<TX2>One of the most notable networking protocols that does not encrypt data in transit is FTP (File Transfer Protocol). FTP is commonly used on the Internet to transfer files. You have probably used it many times when you have downloaded software. In this lab, you install an FTP server and a protocol analyzer.

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

* Install and configure the FTP service on Windows Server 2016
* Install and configure the protocol analyzer Wireshark

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Completion of Lab 4.1
* Windows 10 VM

**<H2>Activity**

<FE1TX1>Estimated completion time: **20–30 minutes**

<TX1>In this lab, you install and configure an FTP server on Windows Server 2016 and download and install the protocol analyzer Wireshark.

1. <NL\_FIRST>Log on to Windows Server as Administrator.
2. <NL\_MID>If necessary, click the Server Manager icon on the task bar.
3. Click Manage, then click Add Roles and Features, and click Next at the Before You Begin window. In the Installation Type window, click Next. In the Server Selection window, click Next.
4. In the Server Roles window, place a check mark in the box to the left of Web Server (IIS), and in the Add Roles and Features wizard, click Add Features.
5. Click Next three times, and in the Role Services window, scroll down and expand the FTP Server, and place a check mark in the FTP Service check box.
6. Click Next.
7. Click Install.
8. When the installation has completed, click Close in the Roles and Features Wizard dialog box.
9. In Server Manager, click Tools, then click Internet Information Services (IIS) Manager. If necessary, click No in the Internet Information Services (IIS) Manager dialog box.
10. You must configure your IIS server to handle FTP protocols. In the Server Manager Dashboard, click Add roles and features.
11. If the Before you begin page of Add Roles and Features Wizard is displayed, click Next.
12. On the Select installation type page, select Role-based or feature-based installation, and click Next.
13. On the Select destination server page, click Select a server from the server pool, select your server from the Server Pool list, and then click Next.
14. On the Select server roles page, expand the Web Server (IIS) node, and then expand the FTP Server node.
15. If necessary, select the FTP Server check box and the FTP Service check box, and then click Next.
16. If necessary, on the Select features page, click Next.
17. If necessary, on the Confirm installation selections page, click Install.
18. On the Windows server, create a folder named **FTP Data** on the C: drive. Within that folder, create a file called **Credentials.txt** that contains your name and the current date.
19. Open the IIS Manager dialog box and expand the **Windows** Server node. Right click the **Sites** node and select **Add FTP site**.
20. In the FTP site name text box, enter **FTP Data**. In the Physical Path, navigate to the FTP Data folder you created in step 19. Click **Next**.
21. Notice in the Bindings and SSL Settings window that the FTP server will be listening for requests for FTP service at TCP port 21, the standard FTP control port. In the IP Address drop down, select the server’s IP address. Select the **No SSL** option and click **Next**.
22. Select **Basic** and **Anonymous** in the Authentication area.
23. In the Authorization area, select **All users** from the dropdown and verify that Permissions are set to both Read and Write. Click **Finish.**
24. In the search box type **wf.msc** to open Windows Firewall. Turn off the firewall for Domain, Private, and Public. Click **Apply** and then **OK**.
25. Log on to Windows 10 VM with an administrative account.
26. Open your web browser and go to <URL>www.wireshark.org</URL>.

[BEGIN NOTE]

<B1TX1>It is not unusual for websites to change where files are stored. If the suggested URL no longer functions, open a search engine such as Google and search for “Wireshark”.

[END NOTE]

1. Click the Download—Get Started Now button. On the Download Wireshark page, click Windows Installer (*XX*-bit) where *XX* is the numbers of bits for your version of the OS. In the File Download window, click Save and save the file to your desktop.
2. In the Download complete window, click Run, and if you receive a warning stating that the publisher could not be verified, click Run again. If necessary, click **Yes** on the User Account Control Dialog.
3. Click Next on the Welcome to the Wireshark Setup Wizard page, click I Agree at the License Agreement page, accept the default components on the Choose Components page, and click Next. Accept the default settings on the Select Additional Tasks page and click Next, accept the default Destination Folder and click Next, and then accept the default settings on the Install WinPcap page and click Install.
4. Click Next at the Welcome to the WinPcap Setup Wizard page, click Next again, and then click I Agree at the License Agreement page.
5. Click Install, click Finish at the Completing the WinPCap Setup Wizard, click Next, and then click Finish on the final page.
6. Close all windows and log off.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.6 Given a scenario, implement secure protocols.
* 3.1 Explain use cases and purpose for frameworks, best practices, and secure configuration guide.

**<H2>Review Questions**

1. <MULT>Your Windows Server 2106 is named server02.acme.com. It is running the FTP server service. While reviewing the FTP logs, you notice entries indicating that a user named IUSR\_SERVER02 has been logging on and accessing the FTP directory. What is the significance of these log entries?
   1. **<MULTA>Anonymous access is permitted by your FTP server.**
   2. Users from the Internet have accessed your FTP server.
   3. Log maintenance has been performed by the IUSR service.
   4. It is likely that your system has been attacked.
2. <MULT>Which of the following is a capture file format that can be read by Wireshark? (Choose all that apply.)
   1. **<MULTA>Microsoft Network Monitor captures**
   2. Cisco Secure Ingress Log output
   3. **Novell LANalyzer captures**
   4. **tcpdump**
3. <MULT>Which of the following statements best describes the function of WinPcap?
   1. <MULTA>WinPcap provides the logging functions for Wireshark.
   2. **WinPcap allows applications to capture and transmit network packets bypassing the protocol stack.**
   3. WinPcap is a device driver that allows applications to communicate with the Windows operating system.
   4. WinPcap adds functionality to Wireshark, including skins, fonts, extended color depth, and advanced rendering.
4. <TF>In a Windows Server 2106 FTP server, configuration options in the FTP site’s Properties/Directory Security permit administrators to block specific computers from connecting with the FTP server based on the client’s IP address or NetBIOS name. True or **False**?
5. <MULT>You have decided to track user activity on your Windows Server 2106 FTP server by storing your FTP log file information on a Microsoft Access database. What would be the most sensible choice of formats in which to save your FTP log files?
   1. <MULTA>W3C Extended Log File Format
   2. **ODBC logging**
   3. Microsoft IIS Log File Format
   4. Comma Separated Value Format

# <H1>Lab 9.3 Capturing and Analyzing FTP Traffic

**<H2>Objectives**

<TX1>FTP is a commonly used protocol. On some websites from which software can be downloaded, users are given the option of using HTTP or FTP as the download protocol. On others, the user is automatically switched to FTP to receive the download. Most web browsers allow the use of HTTP or FTP in the address bar. For example, if you wanted to connect to an FTP server called ftp.acme.com, you could type the following in the web browser address bar: ftp://ftp.acme.com. Note that it is the service identification (http:// or ftp://) that determines the protocol used and service accessed, not the “www” or the “ftp” that are found in many fully qualified domain names. If an FTP server were named files.acme.com, it could be accessed in a web browser by entering ftp://files.acme.com.

<TX2>FTP software is frequently used by webpage administers to upload webpages and files. Note that in all these applications of FTP, the data are traversing the Internet in the clear. Because confidential information is not sent, there is no real security risk in downloading software using FTP (unless, of course, the software is malicious). However, web administrators who send their authentication credentials during their webpage uploads should not be surprised if their website is targeted for defacement or worse. In this lab, you capture and analyze FTP traffic.

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

* <BL>Capture network traffic with Wireshark
* Analyze captured FTP traffic

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>The successful completion of Lab 9.2

**<H2>Activity**

<FE1TX1>Estimated completion time: **30–60 minutes**

<TX1>In this lab, you use a protocol analyzer to capture FTP traffic and analyze the results.

1. <NL\_FIRST>Log on to Windows 10 VM as the administrator.
2. <NL\_MID>Click Start, type WireShark, and then click the Wireshark program.
3. Select the ethernet controller you wish to capture packets from.
4. Click the Start button. Unless there is no network traffic, you will see frames, appearing as rows, added to your screen. If you are on a switched network, you will not see all the traffic on the network. Focus on the communication between Windows 10 VM and Windows Server. On the Capture menu, click Stop so you can set up your connection to the FTP server.
5. Start the Wireshark capture.
6. Open a command prompt, type cd \, and press Enter.
7. Type ftp IP address of Windows Server and press Enter.
8. Log into the FTP server (See Figure 9-3) using the administrator account credentials.

**[Insert Figure 9-3 Here]**

1. Log on to the FTP server as mbloom. (If you have not previously created this user, In Server Manager, click Tools, then click Active Directory Users and Computers, expand your domain, right-click the Users container, click New, and click User. Create a user with the full name Molly C Bloom, the User login name mbloom, and the password Pa$$word.) Press Enter.
2. Type Molly Bloom’s password as Pa$$word and press Enter.

[BEGIN NOTE]

<B1TX1>If too much time elapses between entering the username and entering the password, the system rejects the access attempt. If this happens, type **bye,** press **Enter**, and try the ftp *IP Address* command again.

[END NOTE]

1. At the ftp> prompt, type dir and press Enter to see what files are in the FTP server’s home directory. If you get a Windows Firewall error, click Unblock and click Continue at the User Account Control window. You should now see the file Confidential.txt listed.
2. Download Confidential.txt to your C: drive as follows: Type get Confidential.txt and press Enter.
3. Type bye and press Enter to disconnect from the FTP server; return to Wireshark and, from the Capture menu, click Stop.
4. Click the Windows Start button, click Computer, navigate to C:\Users\Administrator.Team1\Confidential.txt and open it to verify that you downloaded it successfully.
5. Return to Wireshark and examine the captured packets.
6. If, in the Source and Destination columns, you see a lot of IP addresses or MAC addresses that don’t belong to your Windows 10 VM or your FTP server, click **Capture** and then select **Capture Filters**. This opens the dialog box shown in Figure 9-4, where you can filter the addresses Wireshark is listening for.

**[Insert Figure 9-4 Here]**

1. Examine the frames and look at the Info column for clues to the purpose or content of the frame; keep an eye on the ASCII representation of the data portion of the frame in the lower window (see Figure 9-5). What parts of the FTP session would be readable to an attacker sniffing the network with a protocol analyzer like Wireshark?

**[Insert Figure 9-5 Here]**

1. Return to the Windows Server and restore Windows Firewall to its original settings.
2. Close Wireshark without saving the capture. Close all open windows and log off.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>1.5 Explain vulnerability scanning concepts.
* 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.
* 2.6 Given a scenario, implement secure protocols.
* 3.2 Summarize various types of attacks.

**<H2>Review Questions**

1. <MULT>You have been asked to install an FTP server on the company’s internal network, to be used only by an employee committee that will be working on an advertising campaign to encourage employees to donate to a charity. Which of the following would be the most secure configuration of the FTP server?
   1. <MULTA>Require users to authenticate using their domain account.
   2. Require users to authenticate using a local account.
   3. **Require users to use anonymous authentication.**
   4. Allow users to share a single username and password.
2. <MULT>In this lab, what is listed in the Info column of the frame in which the content of the file Confidential.txt is visible?
   1. **<MULTA>FTP Data**
   2. Response
   3. Request
   4. get-request
3. <MULT>Which of the following statements is the most accurate description of the communication between Windows 10 VM and the FTP server in this lab?
   1. <MULTA>Windows 10 VM initiated the connection by sending to the FTP server a packet with TCP flags SYN and ACK set.
   2. Windows 10 VM initiated the connection by sending to the FTP server a packet with TCP flag ACK set.
   3. **Windows 10 VM initiated the connection by sending to the FTP server a packet with TCP flag SYN set.**
   4. The FTP server initiated the connection by sending a packet to Windows 10 VM with TCP flag SYN set.
4. <MULT>Which of the following statements is the most accurate description of the communication between the Windows 10 VM system and the FTP server in this lab?
   1. **<MULTA>Once the FTP server was contacted by Windows 10 VM, it sent a packet with the TCP flags SYN and ACK set.**
   2. Once the FTP server was contacted by Windows 10 VM, it sent a packet with the TCP flag ACK set.
   3. Once the FTP server was contacted by Windows 10 VM, it sent a packet with the TCP flag SYN set.
   4. The FTP server was not first contacted by Windows 10 VM; it advertised its FTP service, and Windows 10 VM responded.
5. <MULT>Which of the following statements is the most accurate description of the communication between the Windows 10 VM system and the FTP server in this lab?
   1. <MULTA>The teardown of the TCP session began when the FTP server sent a packet to Windows 10 VM with the TCP flag FIN set.
   2. **The teardown of the TCP session began when Windows 10 VM sent a FIN packet to the FTP server.**
   3. The teardown of the TCP session began when the FTP server sent a packet to Windows 10 VM with the TCP flags FIN and ACK set.
   4. The teardown of the TCP session began when Windows 10 VM sent a packet to the FTP server with the TCP flags FIN and ACK set.

# <H1>Lab 9.4 Physical Security Planning

**<H2>Objectives**

<TX1>You have been brought in as a consultant to a software engineering company that is planning its new office building. They are extremely concerned with the layout of the office and ask for advice on making it more physically secure. The floor plan for the building is shown in Figure 9-6.

**[Insert Figure 9-6 here]**

You need to suggest alterations to the floor plan that will improve physical security, disaster recovery options, security controls, server room options, door security controls, and any other internal/external security that may be needed.

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

* <BL>Determine exterior controls for a building
* Determine physical controls for a building
* Analyze a business’s physical security features

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>A computer with a word processor

**<H2>Activity**

<FE1TX1>Estimated completion time: **30–60 minutes**

<TX1>In this lab, you analyze the internal and external physical security of a building.

1. <NL\_FIRST>Perform a SWOT analysis of the existing floor plan, and list the following:
   * 1. <LL>Strengths
     2. Weaknesses
     3. Opportunities
     4. Threats
2. <NL\_MID>List any external environmental controls you suggest adding to the building.
3. List any internal environmental controls you suggest adding to the building.
4. What should the network layout look like? Where should access points be stationed and what zones might be introduced into the network?
5. What type of physical controls would you recommend at each workstation or desktop?
6. What features should be incorporated into the server room?
7. Do you recommend a receptionist? A security guard? If so, where should they be positioned?
8. Is every aspect of the office viewable from all other areas? Do you recommend a surveillance system?

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.1 Install and configure network components, both hardware- and software-based, to support organizational security.
* 3.2 Given a scenario, implement secure network architecture concepts.
* 3.9 Explain the importance of physical security controls.
* 5.7 Compare and contrast various types of controls.

**<H2>Review Questions**

* 1. <MULT>Which is not a part of a SWOT analysis?

1. <MULTA>Weaknesses
2. Opportunities
3. Threats
4. **Supervise**
   1. <MULT>When designing the floor plan, what is the best approach for doors that are not at the main entrance?
5. <MULTA>They should open with no security on them.
6. They should be locked at all times with no means of opening them.
7. **They should be locked with either a key pad entry or a door code system**
8. There should be a guard posted at each door.
   1. <TF>Computer cables are not needed in cubicles because there is security at the front door. True or **False**?
   2. <MULT>What mechanism should be positioned facing a server closet door, if the closet door is not in the employees’ direct line-of-sight?
9. **<MULTA>A camera recording all entry and exit from the room.**
10. A security guard
11. A do not disturb sign
12. A enter at your own risk sign
    1. <TF>All the computers in the building should be in one network zone. True or **False**?

# <H1>Lab 9.5 Data Loss Prevention

**<H2>Objectives**

<TX1>In general, more information security problems are caused by internal users than by external attackers. After all, internal users have access to company data and are authorized to perform data manipulation and transmission. Errors are bound to occur, and there is the danger that even an honest employee will take data out of the office, not to mention the danger that a dishonest employee will remove the organization’s intellectual property. Taking data in laptops or flash drives is not the only danger. Users can also transmit sensitive data through email and other network services. This type of data loss can be intentional or unintentional. Given the ease with which data can be moved, how can a company know where its data are? This question is particularly important to organizations that deal in personally identifiable information, such as medical records or client financial information. Federal and state regulators have become more and more interested in protecting the privacy of consumers, and companies are required to account for the location of these data.

<TX2>Information security vendors have responded to these problems with products called data loss prevention systems. The name is a little misleading because the systems are often set to monitor data locations and data movement rather than prevent data movement and storage, but many of these products are capable of taking action when it is determined that data are being placed out of the organization’s control. In this lab, you learn more about data loss prevention.

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

* <BL>Explain the need for data loss prevention
* Discuss data loss prevention methods
* Discuss advantages and disadvantages of data loss prevention solutions

**<H2>Materials Required**

<H1>This lab requires the following:

* <BL>A PC with Internet access

**<H2>Activity**

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

<TX1>In this lab, you research data loss prevention.

1. <NL\_FIRST>Open your web browser and go to <URL>http://www.sans.org/reading-room/whitepapers/dlp/data-loss-prevention-32883</URL>.

[BEGIN NOTE]

<B1TX1>It is not unusual for websites to change where files are stored. If the suggested URL no longer functions, open a search engine such as Google and search for “Prathaben Kanagasingham and data loss prevention”.

[END NOTE]

1. <NL\_MID>Read the article on data loss prevention by Prathaben Kanagasingham.
2. Answer the Review Questions that follow.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.1 Install and configure network components, both hardware- and software-based, to support organizational security
* 3.3 Given a scenario, implement secure systems design
* 3.7 Summarize cloud and virtualization concepts
* 3.8 Explain how resiliency and automation strategies reduce risk
* 5.6 Explain disaster recovery and continuity of operation concepts

**<H2>Review Questions**

* 1. <FIB>A regular expression is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

1. <FIBA>data not considered sensitive
2. data transmitted through a network on a regular basis
3. a security policy that defines the implementation level of data loss prevention
4. **a method of expressing a search pattern**
   1. <MULT>Which of the following is considered structured data?
5. <MULTA>A resume
6. **A phone number**
7. An email
8. A receipt
   1. <FIB>Data loss prevention methods that monitor the data leaving a workstation via a flash drive require \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
9. <FIBA>software that blocks physical ports
10. **an agent-based approach**
11. the cooperation of the workstation user
12. technologies that transmit the workstation user’s keystrokes in real time
    1. <FIB>When phasing in a data loss prevention solution, most organizations start by monitoring \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
13. <FIBA>data at rest
14. **data in motion**
15. end-point data
16. data at rest, data in motion, and end-point data simultaneously
    1. <FIB>Mr. Kanagasingham states that implementation of data loss products will require additional IT staff because of the need to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (Choose all that apply.)
17. <FIBA>respond to user questions
18. **respond to false positives**
19. **initiate escalation**
20. initiate product testing