<CHN>CHAPTER FOURTEEN

<CHT>BUSINESS CONTINUITY

<COOT>Labs included in this chapter

* <COOH1>Lab 14.1 Installing VMware Player
* Lab 14.2 Adding Hard Drives to a Virtual Machine
* Lab 14.3 Creating RAID
* Lab 14.4 Creating Fault Tolerant RAID
* Lab 14.5 Comparing a System’s Current State to Its Baseline State

<COOBT>CompTIA Security+ Exam Objectives

**<COOBL>Domain Lab**

<COOB>Threats, Attacks, and Vulnerabilities 14.5

Technologies and Tools 14.5

Architecture and Design 14.1, 14.2, 14.3, 14.4

Risk Management 14.1, 14.2, 14.3, 14.4

# <H1>Lab 14.1 Installing VMware Player

**<H2>Objectives**

<TX1>There are many different types of virtualization software. So far in this lab manual, you have been using VirtualBox. This lab explores VMware Player, which acts as the interface between the guest operating system and the physical hardware on the host computer. The guest operating system “thinks” that it is running on real hardware, and most of the time it behaves exactly as it would if it were installed on the actual computer. If the host computer has enough RAM, it can run multiple virtual operating systems simultaneously. In this way, a virtual network can be created. These features make virtual machines ideal for training and testing, as you will be doing in this chapter.

<TX2>Virtualization has many other uses as well. Technical support analysts can easily pull up the same operating system that the customer is using. Developers can test software on multiple systems. And multiple servers can be running on one physical server. Running them on one server reduces hardware costs and utility bills and saves rack space in the data center.

<TX2>Virtualization is also an asset in disaster recovery and business continuity. A virtual server can be migrated from one physical machine to another while still providing availability of data, a keystone of a business continuity policy. The hardware independence of virtualization allows quick recovery because the exact hardware of the system being restored does not have to be duplicated.

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

* <BL>Install and configure VMware Player
* Install a guest operating system

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows 10

**<H2>Activity**

<FE1TX1>Estimated completion time: **35 minutes**

<TX1>In this lab, you will install VMware player, and then change the default settings of the virtual hard drive.

1. <NL\_FIRST>Log on to Windows 10 VM with an administrative account.
2. <NL\_MID>Open Internet Explorer and go to <URL>https://www.vmware.com/products/workstation.html.</URL>

**[Insert Icon Here]**

<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 “VMware Player.”

1. Scroll down to Workstation Player or Workstation Pro, and then click Download Now under Workstation Player. If necessary, choose the version of Workstation player that fits your machine requirements. Save the file to your desktop.
2. Double-click the exe file download in the step 3 file. If necessary, click Yes on the User Account Control Dialog, and then click Next.
3. Select I accept the terms **in the License Agreement**, then click Next. Confirm the destination folder, and then click Next.
4. Uncheck the **Check for product updates on startup** box, Uncheck **Help improve VMware Workstation Player**, then click Next.
5. Click Next on the Shortcuts window, then click Install. When the installation is complete, click Finish.
6. Launch VMware Player, enter a valid email address in the first dialog box, click Continue, then click Finish.
7. Click Create a New Virtual Machine.
8. Select I will install the operating system later, then click Next.
9. Select the Windows 10 instance in the OS list, then click the Player menu, then click Manage, then click Virtual Machine Settings.
10. Click through the hardware options and note the default settings.
11. Click Next three times, then click Finish.
12. Shut down the VMware Player.
13. Log off the host machine.

<H2>Certification Objectives

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>3.2 Given a scenario, implement secure network architecture concepts.
* 5.3 Explain risk management processes and concepts.

<H2>Review Questions

1. <MULT>The default hard disk type for creating a new virtual hard disk is?
2. <MULTA>SATA
3. **SCSI**
4. USB
5. Virtual
6. <MULT>A disk image file has what extension?
7. <MULTA>Java
8. Doc
9. **ISO**
10. Exe
11. <MULT>By default, how many processors does an instance of VMware Player default to?
12. **<MULTA>1**
13. 2
14. 3
15. 4
16. <TF>If the machine has unlimited resources, there is no maximum number of virtual machines that can be run on a computer. **True** or False?
17. <MULT>What is the maximum amount of memory that can be allocated to a virtual machine?
18. <MULTA>1 GB
19. 2 GB
20. 3 GB
21. **It depends on the machine that is hosting the software**

# <H1>Lab 14.2 Adding Hard Drives to a Virtual Machine

<H2>Objectives

<TX1>A great benefit of using virtualized operating systems is that you can add virtual hardware. For example, you can add additional NICs, enable IP routing, and create a virtual router. As you will find out in this lab, virtual hard drives can be added without opening the computer chassis. You do not have to open the computer and work in tight spaces to attach cables and mount drives; no one has ever dropped a screwdriver and damaged a motherboard while installing a virtual hard drive.

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

* <BL>Install and configure virtual hard drives
* Describe the difference between basic and dynamic disks

<H2>Materials Required

<TX1>This lab requires the following:

* <BL>Windows 10
* Successful completion of Lab 14.1

<H2>Activity

<FE1TX1>Estimated completion time: **10–15 minutes**

<TX1>In this lab, you will create two virtual hard drives and associate them with a virtual machine.

1. <NL\_FIRST>Log on to your Windows 10 machine with an administrative account.
2. <NL\_MID>Launch VMware Player.
3. Select the Windows 10 instance in the OS list, then click the Player menu, then click Manage, then click Virtual Machine Settings.
4. Click the Add button at the bottom of the hardware options window.
5. Select Hard Disk from the Hardware types window, then click Next.
6. Choose the recommended Virtual disk type, then click Next.
7. Choose Create a new virtual disk, then click Next.
8. Click Next, then rename the file to a name of your choice or a name given by your instructor, then click Finish.
9. Notice that a second hard disk appears in the Hardware list. If you click on the hard disk you can change its settings.
10. Repeat Steps 3–7 to create a second virtual drive with the same characteristics.
11. Log off the host computer.

<H2>Certification Objectives

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>3.2 Given a scenario, implement secure network architecture concepts.
* 3.7 Summarize cloud and virtualization concepts.
* 5.3 Explain risk management processes and concepts.

<H2>Review Questions

1. <MULT>Which of the following statements regarding the Basic and Dynamic disks is correct?
2. <MULTA>A dynamic disk that contains data cannot be reverted to a basic disk.
3. A basic disk that contains the operating system partition(s) cannot be converted to a dynamic disk.
4. To revert a dynamic disk that contains data to a basic disk without losing data, a mirrored drive must be created and then, after the reversion, the mirrored drive is used to regenerate the mirrored set.
5. **To revert a dynamic disk that contains data to a basic disk without losing the data, a backup of the dynamic disk must be made and, after the reversion to a basic disk, the data must be restored from the backup medium.**
6. <TF>Basic disks support only four partitions because there is not enough space in the partition table to identify more. Dynamic disks support more than four volumes per disk because the table that tracks volumes is much larger than the partition table on a basic disk. **True** or False?
7. <MULT>You intend to upgrade a Windows 2003 Server file server to Windows Server 2016. The Windows 2003 server has three hard drives. The first two (dynamic disks) are a mirrored array of the operating system. The third drive (basic disk) contains user files. Because there is no free or unallocated space left on the third drive, you will replace this drive with a larger one after the system upgrade. Using the Windows Server 2016 DVD, you successfully complete the upgrade. After the final reboot, you open the Computer Management console, but when you attempt to upgrade Disk 3 to a dynamic disk, the process fails. What is the most likely reason for this failure?
8. **<MULTA>There is not enough unallocated space on Disk 3.**
9. You are not logged on with an administrative account.
10. On a single system, all disks must be converted from Basic to Dynamic disks at once.
11. Disk 3 is formatted with NTFS.
12. <MULT>Which of the following statements regarding the Microsoft system and boot partitions is correct? (Choose all that apply.)
13. **<MULTA>The system partition contains the files required for the system to boot.**
14. **The boot partition contains the operating system files.**
15. **The boot partition and the system partition can be installed on separate hard drive partitions.**
16. **The boot partition and the system partition can be installed on a single hard drive partition.**
17. <MULT>Which of the following statements regarding volumes is correct? (Choose all that apply.)
18. **<MULTA>A simple volume can be made smaller to make room for another volume on the same disk.**
19. **A simple volume can be enlarged by adding a new hard disk and creating a spanned volume.**
20. **A simple volume can be enlarged by creating an expanded volume.**
21. A simple volume cannot be reformatted once it has been formatted in NTFS.

# <H1>Lab 14.3 Creating RAID

<H2>Objectives

<TX1>Redundancy is the most common way to provide fault tolerance. As an example, most companies that rely on wide area network (WAN) connections have redundant WAN links. They might use Asynchronous Transfer Mode (ATM) for normal traffic and a digital subscriber line (DSL) connection in case the main WAN link goes down, or the company may contract with two different T-carrier providers because it is unlikely that a service outage will hit both providers at once. Servers can be built with redundant power supplies and redundant cooling fans, and a LAN can be connected to a WAN with parallel (redundant) routers. Furthermore, when mission-critical business data are stored on hard drives, Redundant Array of Independent Disks (RAID) can keep the data flowing despite a disk crash because parity (encoded information that can be processed to provide the data contained on the “lost” disk) is stored on the remaining disks.

<TX2>The main three types of RAID are RAID 0, RAID 1, and RAID 5. Here are descriptions of each:

* <BL>RAID 0, also called a striped set or striped volume, consists of multiple hard drives that act as a single volume. As a file is saved, some is written to drive 0, some to drive 1, some to drive 2, and so on. The main benefit of this type of RAID is performance. When a file is called up from a RAID 0 set, the controller on drive 0 can start sending the first part of the file to the central processing unit at the same time that drive 1’s controller is loading the next part of the file. If the file was written on a single disk, the file would have to be read in sequence rather than in “parallel.” The problem with RAID 0 is that if a disk fails, all the data on the array are lost. RAID 0 is not really RAID in that it is not redundant.
* RAID 1, also called a mirrored set or mirrored volume, is clearly redundant. Any operations performed on one disk simultaneously occur on the second disk, so if one disk fails, the other can take over instantly without any loss of availability. The down side to this approach is the high cost of storage; for every 300 GB of needed storage space, you have to buy 600 GB of hard drive space.
* Another fault tolerant option is RAID 5 where, as in RAID 0, data are striped across a number of disks. Unlike RAID 0, RAID 5 is fault tolerant because, along with the file, the disk controllers write parity—that is, information that can be processed to re-create parts of the file that are lost when a single disk fails. The cost of storage is improved compared to RAID 1 because parity is compressed. For example, a three-disk RAID 5 set, where each drive is 300 GB, provides 600 GB of storage, while 300 GB or one-third of the total space is used for parity. The more disks you add, the cheaper the storage. A four-disk array uses only one-fourth of the total space for parity. However, if more than one disk fails, the data are lost.

<TX2>Why is RAID not considered a backup strategy? If you are using a backup tape to restore a server, the server is not available, and if it is not available, it is not fault tolerant. A common question that students ask is, “Why go to all the trouble of backing up a RAID array when it’s already fault tolerant?” Imagine that your RAID 5 array has been infected by a virus. What good will fault tolerance do (other than to keep an infected system online) when you do not have a tape of yesterday’s data that had not been infected yet?

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

* <BL>Create a RAID set
* Explain the advantages and disadvantages of RAID 0, 1, and 5

<H2>Materials Required

<TX1>This lab requires the following:

* <BL>Windows 10
* Successful completion of Lab 14.2

<H2>Activity

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

<TX1>In this lab, you will create a RAID set and test its level of fault tolerance when a disk fails.

1. <NL\_FIRST>Log on to Windows 10 with an administrative account.
2. <NL\_MID>Open VMware Player and start Windows 10.
3. In the Windows 10 VM, click the Search icon on the task bar, type diskmgmt.msc and press Enter.
4. In the Disk Management console, right-click in the Unallocated space area of Disk 1. Click New Striped Volume.
5. In the Welcome to the New Striped Volume Wizard window, click Next. In the Select Disks window, notice the size of Disk 0 in the Selected box. In the Available box, click Disk 0 and then click the Add button. Notice that the size to be used from Disk 1 has decreased to match that of Disk 0 because all disks in striped volumes must have approximately the same size. Click Disk 2 in the Available box and click Add. Notice that the Total volume size in megabytes is the sum of the three 197 MB drives (your system may show a slightly different number). Your Select Disks window should look like what is shown in Figure 14-1. From this information, can you tell whether this array is redundant? Click Next.

**[Insert Figure 14-1 Here]**

1. In the Assign Drive Letter or Path window, verify that Assign the following drive letter is selected and then use the drop-down menu to select the letter O and click Next.
2. In the Format Volume window, change the Volume label to RAID?, and if necessary, place a check mark in the box to the left of Perform a quick format, and click Next. Click Finish.
3. After a few moments, the RAID? drive is formatted and the color stripe changes to show the type of drive (see the legend at the bottom of the window). Your Disk Management console should now look similar to what is shown in Figure 14-2.
4. Click Start, click Computer, and open the O: drive. Create a folder named Important Docs and, inside Important Docs, make a document named Clients.txt.
5. Close all windows and shut down Windows 10.
6. From VMware Player, select Windows 10 and click Edit virtual machine settings. Click the Hard Disk 2 row, and click the Remove button. This simulates a hard disk crash.

**[Insert Figure 14-2 Here]**

1. Restart Windows 10 and log on with your administrative account.
2. Click Start, click Computer, and access the O: drive. Why were you unable to access the Important Docs folder?
3. Access the Disk Management console. Your console should look similar to what is shown in Figure 14-3.

**[Insert Figure 14-3 Here]**

1. Right-click the Disk 0 box and examine the accessible options. Do the same with Disk 1. Right-click the box identified as Missing (it has a red circle with a white “x”), click Reactivate Disk, and click OK. Because the drive is gone, this will not regenerate the array; there is no disk to reactivate.
2. Shut down Windows 10. Using the techniques shown earlier in this lab, create a new 200 MB virtual hard disk with the filename Replacement.vhd and associate it with virtual Hard Disk 2. Restart Windows 10 and log on with your administrative account.
3. Open the Disk Management console. Initialize the new disk and convert it to a dynamic disk. Right-click the Failed box (volume) on Disk 0, click Reactivate Volume, and then click OK. This fails. Attempt the same tactic on the Failed volume on Disk 1. This, too, fails. Right-click the largest unallocated space on the new disk—that is, Disk 1. There are no options to join this to the existing striped volume, although you can create new volumes. Your Important Docs folder is gone forever, unless you made a backup of it.
4. Right-click either of the failed volumes and click Delete Volume, and then click Yes. Notice that the Missing drive is now gone and Disk 1 is now a basic disk. If the Missing disk is still present, shut down the virtual machine, reboot, and then, from the Disk Management console, right-click the Missing drive and click Remove Disk. Convert all basic disks to dynamic disks.
5. Close all windows and shut down Windows 10.
6. Log off your computer.

<H2>Certification Objectives

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>3.2 Given a scenario, implement secure network architecture concepts.
* 3.3 Given a scenario, implement secure systems design.
* 3.8 Explain how resiliency and automation strategies reduce risk.

<H2>Review Questions

1. <FIB>In the lab, you created a RAID \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ set.
2. **<FIBA>0**
3. 1
4. 5
5. 0 + 5
6. <FIB>In this lab, the Important Documents folder was lost. The main reason for the loss of data was that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
7. **<FIBA>there was no redundancy in the disk array**
8. the disks were formatted using the quick format option, which does not provide the precision required by RAID
9. the Important Documents folder was written to only one disk
10. the replacement disk was installed before reactivating the volume
11. <MULT>Which of the following is an example of fault tolerance? (Choose all that apply.)
12. <MULTA>A spare switch kept in the telecom closet
13. **Multiple domain controllers for a single domain**
14. An uninterrupted power supply connected to a router
15. **Maintaining both on-site and off-site copies of backup tapes**
16. <TF>RAID, as implemented in this lab, results in improved performance. True or **False**?
17. <MULT>Which of the following RAID sets provides the lowest cost per GB of data storage?
18. **<MULTA>RAID 0**
19. RAID 1
20. RAID 5
21. The cost per GB of data storage is equal for all the above.

# <H1>Lab 14.4 Creating Fault Tolerant RAID

<H2>Objectives

<TX1>The RAID implemented in Lab 14.3 was not fault tolerant; it was a RAID 0 set. And although RAID 0 is used primarily for its performance benefits, you did not experience that advantage because the RAID 0 set was implemented on a virtual machine with virtual hard drives. There was only one actual hard drive being used, and only one actual hard drive controller. On the other hand, it was effective in demonstrating how, with RAID 0, the loss of one drive results in the loss of all the data stored on the array.

<TX2>In this lab, you implement a RAID 5 set. Data written to RAID 5 are striped across each of the drives, as is the parity information. Here is a simplified example: a file named Analysis.docx is written to a RAID 5 set that contains three disks. The first part of the file is written to drive 1, and the last part of the file is written to drive 2. On drive 3 is written the parity, which is the information from which the first and second parts of the file can be reconstructed. If drive 3 crashes, all the original Analysis.docx file is present on disks 1 and 2, so the data is still available to users. If drive 1 crashes, the second part of the file is available from drive 2, and drive 3 has the parity information with which to reconstruct the first part of the file. There will be a decrease in performance because reconstruction of data with parity takes more processing than just reading the file directly, but the data remain available despite hardware failure. Of course, if two drives fail, the file cannot be reconstructed.

<TX2>In production environments, RAID 5 is often implemented using 32 hard drives. This enhances performance and decreases storage costs because only 1/32 of the total storage space is used for parity, as opposed to the 1/3 of storage space used for parity in a three-disk array. All hard drives fail at some point, so the chance that one of 32 drives will crash is high enough that the “wasted” 1/32 of storage space is a good investment.

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

* <BL>Configure a RAID 5 set
* Simulate a disk failure and recover the array
* Explain how RAID 5 provides fault tolerance

<H2>Materials Required

<TX1>This lab requires the following:

* <BL>Windows Server 2016 VM
* Successful completion of Lab 14.3
* Successful completion of Lab 4.1
* Creation of 3 dynamic disks

<H2>Activity

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

In this lab, you will create a fault tolerant RAID 5 set, simulate disk failure, demonstrate the continued availability of the resource, and recover the RAID set.

1. <NL\_FIRST>Log on to Windows 10 with an administrative account.
2. <NL\_MID>Open VMware Player and create a Windows Server 2016 VM. Select all the defaults during installation, besides making 2 equal size virtual disks instead of one.
3. Log on to Windows Server 2016 with your administrative account.
4. Open the Disk Management console. Notice that Disk 1 and Disk 2 have a separate 1 MB reserved unallocated space section. Why? Right-click the unallocated section of Disk 1 or 2 and click New RAID-5 Volume.
5. In the Welcome to the New RAID-5 Volume Wizard window, click Next. In the Select Disks window, click Add. Do the same with Disk 2 so that all three disks appear in the Selected box. Can you tell from the Total volume size in megabytes (MB) value whether this is a fault tolerant volume? Click Next.
6. In the Assign Drive Letter or Path window, use the drop-down menu to assign the letter R to the drive and click Next.
7. In the Format Volume window, type RAID! in the Volume label box and place a check mark in the box to the left of Perform a quick format. Click Next and click Finish. After a few moments, the new R volume appears. Close the Disk Management console.
8. Click File Explorer on the task bar, and navigate to the R: drive. Create a folder named Important Docs2 and place a text file named clients2.txt inside the new folder.
9. Right-click the existing hard drive icon in the upper-right corner, then click Settings.
10. In the VMware Player window, click **Windows** Server 2016, and click Edit virtual machine settings. Click the Hard Disk 2 row and, in the left pane, click the Remove button. This simulates a disk crash of one of the RAID-5 disks. Click OK.
11. Boot Server 2016 and log in as Administrator.
12. Open the Disk Management console. Notice the Failed Redundancy warning on the R: drive disks and that Disk 2 is marked as missing. Click File Explorer on the task bar, and navigate to the R: drive. Your data remain available even though one disk is missing.
13. Shut down Server 2016. From the Virtual Machine settings console for Server 2016, create a new 200 MB virtual disk called Replacement2. Associate it with Server 2016’s Disk 2. Boot Server 2016.
14. Log on to Windows Server 2016 with your administrative account.
15. Open the Disk Management console. Initialize the new disk and convert it to a dynamic disk.
16. Right-click the Failed Redundancy volume on Disk 0, and then click Repair Volume. In the Repair RAID-5 Volume window, verify that Disk 2 is selected and click OK. The RAID 5 array will resynchronize. When the R: volume shows a Healthy status, the missing disk no longer is identified as part of the R: drive. Right-click the missing disk and click Remove Disk. The RAID 5 volume is restored.
17. Close all windows and shut down Windows Server 2016.
18. Log off all systems.

<H2>Certification Objectives

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>3.2 Given a scenario, implement secure network architecture concepts.
* 3.3 Given a scenario, implement secure systems design.
* 3.8 Explain how resiliency and automation strategies reduce risk.

<H2>Review Questions

1. <MULT>Which of the following combines fault tolerance with the lowest data storage cost per MB?
2. <MULTA>RAID 0 with 32 disks
3. RAID 1 with 2 disks
4. RAID 5 with 16 disks
5. **RAID 5 with 32 disks**
6. <MULT>Which of the following statements regarding RAID 5 is correct? (Choose all that apply.)
7. The more total disks in an array, the more disks that can fail without loss of data.
8. The fewer total disks in an array, the fewer disks that can fail without loss of data.
9. **The number of disks in the array does not determine the number of disks that can fail without loss of data.**
10. **RAID 5 is fault tolerant.**
11. <TF>Failed redundancy results in loss of data. True or **False**?
12. <FIB>In order to convert a basic disk to a dynamic disk, \_\_\_\_\_\_\_\_\_\_\_\_.
13. <FIBA>there must be at least one dynamic disk already installed on the system
14. **there must be at least 1 MB of unallocated space available on the disk**
15. the disk must be formatted in FAT-32
16. there must be at least 5 MB of unallocated space available on the disk
17. <MULT>A RAID 115 array is a RAID 5 array that has been duplicated on a second RAID 5 array through mirroring. For example, a 16-disk RAID 5 array can be mirrored to another 16-disk RAID 5 array. Which of the following statements regarding a 16-disk RAID 115 implementation is correct? (Choose all that apply.)
18. **<MULTA>One drive can fail without loss of data.**
19. **Two drives can fail without loss of data.**
20. **Four drives can fail without loss of data.**
21. **Six drives can fail without loss of data.**

# <H1>Lab 14.5 Comparing a System’s Current State to Its Baseline State

<H2>Objectives

<TX1>When a server is infected with a rootkit, it can be very difficult to determine whether all elements of the malicious software have been removed and that no files have been corrupted. In these cases, it is usually best to rebuild the system and restore data from backups. However, a danger exists even with this approach because restored systems need to be validated before being returned to service. The validation is needed to confirm that the backups themselves are not infected.

<TX1>One way to perform this validation is to compare the file integrity of the current system to the baseline measurements of a clean system such as a fresh installation. In this lab, you will measure two parameters in the current system and then compare them to the same parameters after the state of the system has been changed.

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

* <BL>Examine a system using Autoruns and Process Explorer
* Compare baseline and current Autoruns and Process Explorer results using WinDiff
* Explain how current state/baseline comparisons can be used to validate a system state

<H2>Materials Required

<TX1>This lab requires the following:

* <BL>Windows 10

<H2>Activity

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

<TX1>In this lab, you will install two utilities with which to create baseline measurements of your system. Then, you will install new utilities and measure the system again to determine if the presence of the new utilities can be detected.

1. <NL\_FIRST>Log on to Windows 10 VM with an administrative account.
2. <NL\_MID>On your desktop, create two folders, one named Autoruns, and one named Process Explorer.
3. Open your web browser and go to <URL>http://technet.microsoft.com/en-us/sysinternals/bb963902</URL>. Click Download Autoruns and Autorunsc. Download the file to the Autoruns folder on your desktop.

**[Insert Icon Here]**

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

1. Return to your web browser and go to <URL>http://technet.microsoft.com/en-us/sysinternals/bb896653</URL>. Click Download Process Explorer. Download the file to the Process Explorer folder on your desktop.

**[Insert Icon Here]**

<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 “process explorer.”

1. Return to your web browser and go to <URL>http://www.grigsoft.com/download-windiff.htm</URL>.

**[Insert Icon Here]**

<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 “windiff.”

Click windiff.zip and save the file to your desktop. Double-click windiff.zip and click Extract all files. In the Select a Destination and Extract Files window, accept the default location, uncheck the box to the left of Show extracted files when complete, and click Extract.

1. Double-click Autoruns.zip in the Autoruns folder on the desktop and click Extract all files. In the Select a Destination and Extract Files window, if necessary, uncheck the box to the left of Show extracted files when complete, and click Extract.
2. Close any open windows or applications. Open the Autoruns folder on your desktop and double-click Autoruns.exe. Click Run in the Open File Security Warning dialog box. In the Sysinternals Software License Terms window, click Agree. Wait until the information bar at the bottom of the window says Ready.
3. Autoruns opens to the Everything tab by default. Explore the other tabs to get a sense of all the drivers (.sys), library files (.dll), services, and other programs that run automatically at boot up. Note that for most items, the applicable registry key is specified.
4. From the File menu, click Save. In the Save AutoRuns Output to File box, navigate to the AutoRuns directory on your desktop, type Baseline\_AutoRuns.txt in the File name box, change the Save as type option to All, and click Save.
5. Double-click ProcessExplorer.zip in the Process Explorer folder on the desktop and click Extract all files. In the Select a Destination and Extract Files window, if necessary, navigate to the Process Explorer folder on your desktop, if necessary, uncheck the box to the left of Show extracted files when complete, and click Extract.
6. Close AutoRuns and any open windows or programs. Open the Process Explorer folder on your Desktop, then double-click procexp.exe. In the Open File—Security Warning dialog box, click Run. If the Sysinternals Software License Terms window appears, click Agree.
7. From the File menu, click **Save As**, and then direct the download to the Process Explorer folder on your desktop. In the File name box, type **Baseline\_Procexp.txt** and press **Enter**. Close the Process Explorer window.
8. Log on as Administrator. Run Autoruns and Process Explorer, as described in Steps 7 through 12, but change the names of the saved files to PostInstall\_Autoruns.txt and PostInstall\_Procexp.txt.
9. Open the Windiff folder on your desktop and double-click WinDiff.exe. Click Run in the Open File—Security Warning dialog box. From the File menu, click Compare Files. Navigate to the Autoruns directory on your desktop and double-click Baseline\_Autoruns.txt. The Autoruns directory will reopen. This time, double-click PostInstall\_Autoruns.txt. A WinDiff file will open, with a single red line that defines the files being compared. Double-click the red line. Your screen will look similar to what is shown in Figure 14-4.

**[Insert Figure 14-4 Here]**

Any items that appear in both the baseline and post install files are shown in white. Any items found in the post install file but not in the baseline file are highlighted in yellow. Determine what items will run at boot up as a result of installing the two utilities. Close WinDiff.

1. Repeat the same procedure, this time comparing Baseline\_procexp.txt and PostInstall\_procexp.txt. Your results should look similar to what is shown in Figure 14-5.

**[Insert Figure 14-5 Here]**

Notice that some items are highlighted in red. These were present in the baseline file but not present in the post install file. As before, the items highlighted in yellow were present in the post install file but not the baseline file, and the items shown in white were found in both files. Examine the highlighted items closely. Are all these items significant? What makes an item significant or insignificant in terms of comparing a system’s current state to its baseline state? Do you think this comparative approach would be an effective way to detect malware? Why or why not?

1. Close all windows and log off.

<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.
* 2.4 Given a scenario, analyze and interpret output from security technologies.
* 5.5 Summarize basic concepts of forensics.

<H2>Review Questions

1. <MULT>Which of the following functions is supported by WinDiff? (Choose all that apply.)
2. **<MULTA>Comparing directories**
3. **Editing files**
4. **Comparing files**
5. Synchronizing files
6. <FIB>Regarding the results of Step 15 of this lab, the presence of a process called \_\_\_\_\_\_\_\_\_\_\_\_ is insignificant. (Choose all that apply.)
7. **<FIBA>SysInternals Process Explorer**
8. PC Tools Auxiliary Service
9. PC Tools Tray Application Service
10. **Hardware Interrupts**
11. <FIB>Regarding the results of Step 14 of this lab, the presence of a program called \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is insignificant. (Choose all that apply.)
12. <FIBA>PCTAVShell Extension
13. sdAuxService
14. **Schedule**
15. **CLFS**
16. <MULT>Which of the following is a method that can be used to validate the restoration of standard operating system files?
17. <MULTA>Antivirus scan
18. **Hashing**
19. Spyware scan
20. Formatting
21. <MULT>Based on your results in this lab, which of the following statements is correct?
22. <MULTA>After initial installation, PC Tools Antivirus must be manually launched in order for the antivirus processes to run.
23. After initial installation, PC Tools Spyware Doctor must be manually launched in order for the antispyware processes to run.
24. After installation of the Google Toolbar, Internet Explorer must be run in order for the Google Toolbar process to run.
25. **After installation, PC Tools Antivirus and PC Tools Spyware Doctor will start on boot up.**