# 1 COMPUTER AND NETWORK SECURITY PRINCIPLES

## PROJECTS

| | |
|---|---|
| **Project 1.1** | Identifying and Analyzing Risk |
| **Project 1.2** | Installing Windows XP Professional |
| **Project 1.3** | Installing Windows Server 2003 |
| **Project 1.4** | Using Microsoft Security Baseline Analyzer |
| **Project 1.5** | Viewing Local Security Policy |
| **Project 1.6** | Creating a Written Security Policy |

| **Project 1.1** | **Identifying and Analyzing Risk** |
|---|---|
| Overview | In this project, you analyze a scenario, identify assets, vulnerabilities, and threats. Next you will calculate risk. You will use the STRIDE threat model to identify potential threats. The STRIDE threat model categorizes threats as follows:<br>▲ Spoofing identifies<br>▲ Tampering with data<br>▲ Repudiation<br>▲ Information disclosure<br>▲ Denial of service<br>▲ Elevation of privilege<br>You will use the DREAD methodology of assessing risk. The DREAD methodology takes into account:<br>▲ Damage potential<br>▲ Reproducibility<br>▲ Exploitablity<br>▲ Affected users<br>▲ Discoverability<br>After the analysis is complete, you will use the following formula to calculate the risks:<br>▲ Risk = Asset x Vulnerability x Threat |
| Outcomes | After completing this project, you will know how to:<br>▲ identify assets<br>▲ Perform qualitative risk analysis |
| What you'll need | To complete this project, you will need:<br>▲ the worksheet below |
| Completion time | 30 minutes |
| Precautions | N/A |

## Scenario:

Busicorp provides a variety of services to small business, including accounting services, advertising services, and web development.

Busicorp allows small business to e-mail accounting records or to upload them to an FTP site. Records are stored in various formats that can be input into Busicorp's accounting software. The accounting software stores records in a Microsoft SQL Server database.

The web development team uses Visual Studio 2005 to build ASP.NET web applications and FrontPage 2005 to build simple informational websites. Developers on the team use either FrontPage or ASP.NET, but not both. Currently all web developers are running Windows XP Professional with Service Pack 2 and Internet Information Services. Customers send the information for their websites through e-mail and also meet with a web designer in person. The web designer has a laptop computer and a USB drive for transferring larger files from the customer's computers. The advertising services team members also have laptop computers. They meet with customers in person to obtain information and to present ideas. Customer contact and billing information is stored in a SQL Server database.

Busicorp's network is a wired LAN with a wireless access point. The laptop computers connect to the network using the wireless access point. The network is an Active Directory domain. The domain controller, the database server, and the e-mail server are located in the IT manager's cubicle. Busicorp has a server with a public IP address that is used as both web server and an FTP server.

## ■ PART A: Identify assets

1. Identify the company's hardware assets:

2. Identify the company's data assets:

3. Which data assets must be kept confidential?

4. Which data assets must be protect from attacks against integrity?

_______________________________________________________________

_______________________________________________________________

_______________________________________________________________

5. What is the impact of a denial-of-service attack on the domain controller?

_______________________________________________________________

_______________________________________________________________

6. On a scale of 1 (lowest) to 5 (highest), rank the following assets in Table 1-1:

**Table 1-1: Asset Ranking**

| **Asset** | **Rank** |
|---|---|
| Customer accounting data | |
| Customer billing data | |
| Customer advertising materials | |
| Customer web applications | |
| User names and passwords | |
| Web/FTP server | |
| Domain controller | |

## ■ PART B: Identify and rank vulnerabilities

1. Five vulnerabilities are listed in Table 1-2. Rank them on a scale of 1 to 5 according to their potential impact on the company. (1 is very little impact and 5 is very large impact).

**Table 1-2: Vulnerability Ranking**

| **Vulnerability** | **Rank** |
|---|---|
| A web designer could lose a USB drive. | |
| The FTP server allows for weak passwords. | |
| Data is transferred to the FTP server in clear text. | |
| The company does not train users on security best practices. | |
| The servers are not in a locked room. | |

2. Add two more vulnerabilities to the table and rank them according to their impact on the company.

## PART C: Identify and rank threats

1. Identify a potential threat for each category in the STRIDE threat model and rank its likelihood on a scale of 1 to 5 (where 1 is least likely) in Table 1-3.

**Table 1-3: Threat Ranking**

| Category | Threat | Rank |
|---|---|---|
| Spoofing identities | | |
| Tampering with data | | |
| Repudiation | | |
| Information disclosure | | |
| Denial of service | | |
| Elevation of privilege | | |

2. Using the ranks you provided in parts A, B, and C, calculate the risk of a user leaving a USB drive at a customer's location. The USB drive has data from another customer on it. The customer where the drive was left replaces the data before returning the USB drive.

3. Using the ranks you provided in parts A, B, and C, calculate the risk of an attacker gaining physical access to the domain controller and unplugging it.

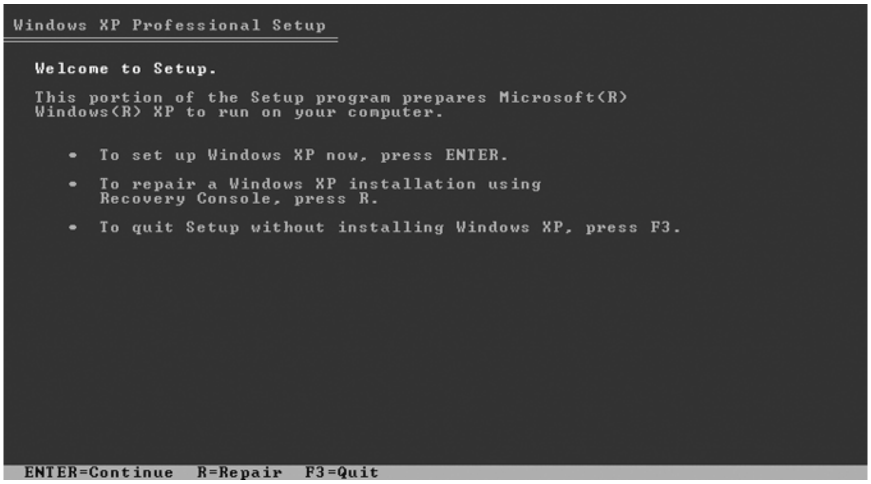
4. Using the ranks you provided in parts A, B, and C, calculate the risk of an attacker obtaining customer accounting data from the FTP site using a dictionary attack to determine the customer's password.

| **Project 1.2** | **Installing Windows XP Professional** |
|---|---|
| Overview | You will use Windows XP Professional for the projects in this book as a client. In this project, you will install Windows XP Professional on one of your computers. |
| Outcomes | After completing this project, you will know how to:<br>▲ install Windows XP Professional<br>▲ view some default security settings |
| What you'll need | To complete this project, you will need:<br>▲ a working computer<br>▲ a Windows XP Professional installation CD-ROM |
| Completion time | 60 minutes |
| Precautions | This lab assumes you are installing Windows XP Professional on a computer without an operating system. It also assumes the computer is on a network with a shared Internet connection. (You will need the Internet connection in Project 1.4)<br>If you are deploying this computer as part of a larger classroom network, your instructor will provide you with alternate instructions for configuring network parameters.<br>If you are adding the computer to an existing network, you must review the project steps with your network administrator. Your network administrator may need to make changes or additions to the installation instructions. |

## ■ PART A: Install Windows XP Professional

Complete the following steps to install Windows XP Professional. These steps assume that there is no operating system currently installed on the computer. You may not understand some of the prompts during installation, but just follow the specific installation instructions provided here.

1. Insert the Windows XP Professional installation CD-ROM in the computer's CD-ROM drive, restart your computer, and then boot from the installation CD. With most computers, you will see a prompt to **Press any key to boot from CD**. Press any key when prompted.
2. When the **Welcome to Setup** screen appears, press Enter to start the installation (Figure 1-1).



```
Windows XP Professional Setup

  Welcome to Setup.

  This portion of the Setup program prepares Microsoft(R)
  Windows(R) XP to run on your computer.

      •  To set up Windows XP now, press ENTER.

      •  To repair a Windows XP installation using
         Recovery Console, press R.

      •  To quit Setup without installing Windows XP, press F3.

  ENTER=Continue   R=Repair   F3=Quit
```

**Figure 1-1: Windows XP Welcome to Setup screen**

3. The **License Agreement** screen opens. Scroll down to the bottom of the page and press F8 to accept the License Agreement.
4. Unless otherwise specified by your instructor, when prompted to select an installation destination, press Enter to accept the default destination.
5. If prompted, press C to continue the installation. This prompt only appears if there is an operating system already installed on the computer
6. When prompted to choose your format option, select to format the partition using the **NTFS** file system and press Enter to start the format.
7. If prompted, press F to verify your selection and start the physical format. Depending on the hard disk size, the format process may take several minutes. After format is complete, Setup will automatically copy the installation files to the hard disk and restart the computer. You can remove the installation CD at this time. DO NOT choose to boot from the installation CD. Installation will continue after the computer restarts from the hard disk.
8. The **Regional and Language Options** screen opens. Verify that the settings are correct and click Next to continue.
9. The **Personalize Your Software** screen appears. Type your name and the name **Busicorp** as the organization name and click Next to continue.
10. The **Your Product Key** screen appears. Enter the product key value for this copy of Windows XP Professional and click Next to continue. If you using an evaluation copy, you will not be prompted for the product key.
11. The **Computer Name and Administrator Password** screen opens. Unless provided with an alternate computer name by your instructor or network administrator, enter the following information and then click Next to continue:

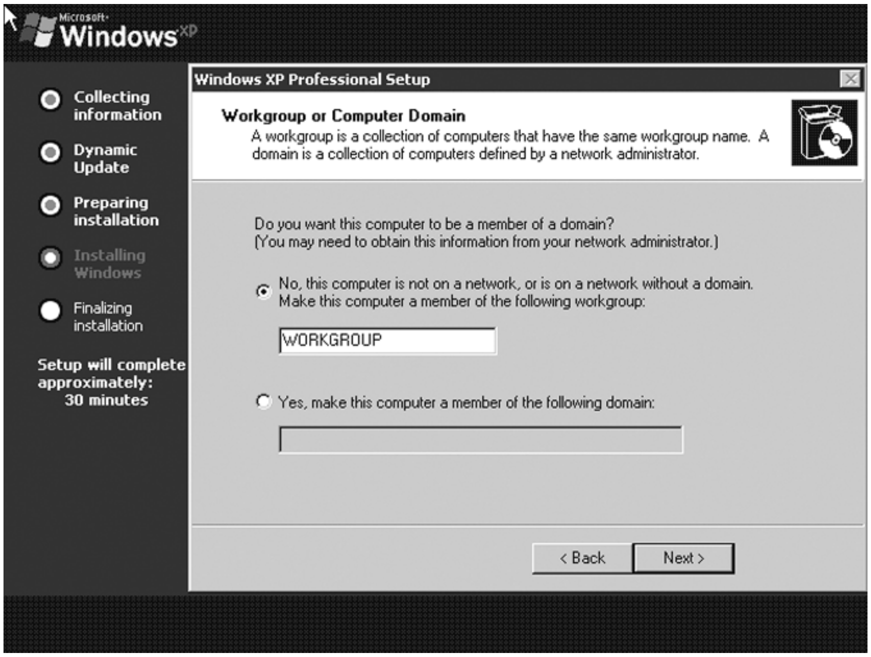
    Computer name: **SECURECLIENT**

12. What change to the installation program would have made Windows XP Professional more secure by default?

____________________________________________________________

____________________________________________________________

13. If you have a Plug and Play modem installed, the **Modem Dialing Information** screen will appear. Specify the settings for your environment and click Next.
14. Select your local time zone in the **Date and Time Settings** screen and click Next to continue. There will be a delay while the computer prepares to install networking.
15. The **Network Settings** screen opens. When prompted for network settings, accept the default **Typical Settings** and click Next**.**
16. The **Workgroup or Computer Domain** screen appears (Figure 1-2). Select the **No, this computer is not on a network, or is on a network without a domain** option button, if necessary, to indicate that you do not want to join a domain. Type **BUSICORPWG** as the workgroup name and click Next to continue. The computer will restart automatically when setup is complete.



Setup will complete approximately: 30 minutes

Windows XP Professional Setup

Workgroup or Computer Domain

A workgroup is a collection of computers that have the same workgroup name. A domain is a collection of computers defined by a network administrator.

Do you want this computer to be a member of a domain?
(You may need to obtain this information from your network administrator.)

● No, this computer is not on a network, or is on a network without a domain.
Make this computer a member of the following workgroup:

WORKGROUP

○ Yes, make this computer a member of the following domain:

Figure 1-2: Workgroup or Computer Domain screen

17. If a dialog box appears reporting that Windows will automatically adjust your screen resolution, click OK. If you can read the text in the next dialog box that is displayed, click OK.
18. The **Welcome to Microsoft Windows** screen appears. Click Next.
19. Type your name in the **Your name** field and click Next.

20. What potential security hole did you just create?

______________________________________________________________________

______________________________________________________________________

21. Click Finish.

## ■ PART B: View default security settings

1. Open **My Computer**.
2. Right-click the **C:** drive and choose **Sharing and Security**.
3. What Windows XP Professional configuration increases security for a new installation?

______________________________________________________________________

______________________________________________________________________

4. Click Cancel.
5. Open the **C:** drive and double-click the **Windows** folder.
6. How does hiding the contents of the system folder improve security?

______________________________________________________________________

______________________________________________________________________

7. Close **My Computer**.

| **Project 1.3** | **Installing Windows Server 2003** |
|---|---|
| Overview | You will use Windows Server 2003 as a server for the projects in this book. In this project, you will install Windows Server 2003 on one of your computers. You will also review some security configuration settings to see how it is secure by default. |
| Outcomes | After completing this project, you will know how to:<br>▲ install Windows Server 2003 |
| What you'll need | To complete this project, you will need:<br>▲ a working computer<br>▲ a Windows Server 2003 installation CD-ROM |
| Completion time | 60 minutes |
| Precautions | This project assumes you are installing Windows Server 2003 on a computer without an operating system. It also assumes the computer is on a network with a shared Internet connection (You will need the Internet connection in Project 1.4). |

If you are deploying this computer as part of a larger classroom network, your instructor will provide you with alternate instructions for configuring network parameters.

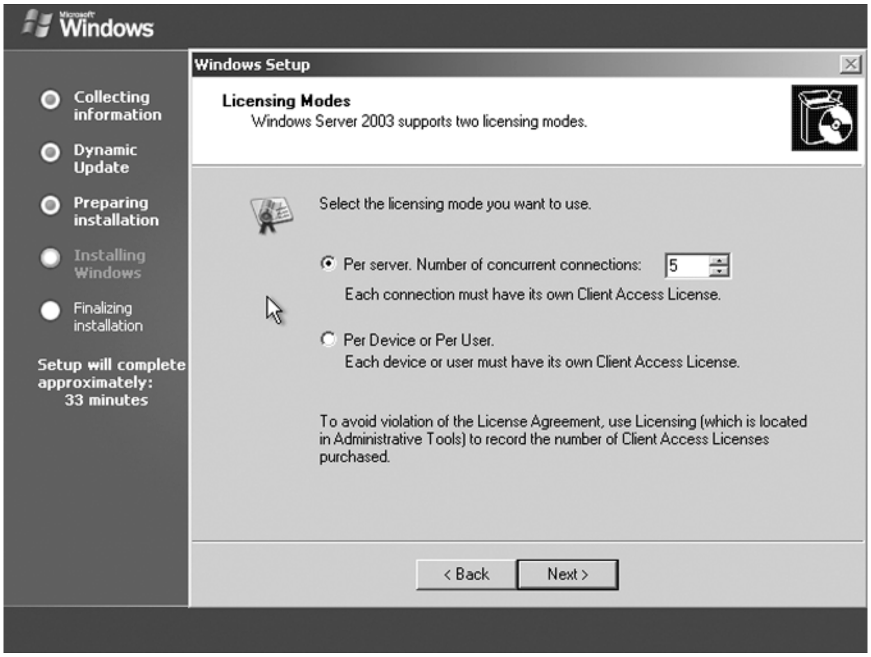
If you are adding the computer to an existing network, you must review the project steps with your network administrator. Your network administrator may need to make changes or additions to the installation instructions.

## ■ PART A: Install Windows Server 2003

Complete the following steps to install Windows Server 2003. These steps assume that there is no operating system currently installed on the computer. You may not understand some of the prompts during installation, but just follow the specific installation instructions provided here.

1. Insert the Windows Server 2003 installation CD, restart your computer and boot from the installation CD. With most computers, you will see a prompt to **Press any key to boot from CD**. Press any key when prompted.
2. When the **Windows Server 2003 Setup** screen opens, the edition you are installing (Standard, Enterprise, Web, etc.) is shown. Depending on the licensing arrangement, you may also see a message telling you that you have only a certain period time in which to activate the installation. Press Enter. The Setup program then begins loading the necessary files for the GUI portion of the installation.
3. After the files have loaded, the **Welcome to Setup** screen appears. When prompted, press Enter to start the installation.
4. The **Windows Licensing Agreement** screen opens. Press F8 to accept the License Agreement.
5. Unless otherwise specified by your instructor, when prompted to select an installation destination, press Enter to accept the default destination.
6. If prompted, press C to continue the installation. You should only see this if there is an operating system already installed on the computer.
7. When prompted to choose your format option, select to format the partition using the **NTFS** file system and press Enter to start the format.
8. If prompted, press F to verify your selection and start the physical format. Depending on hard disk size, the format process may take several minutes. After format is complete, Setup will automatically copy the installation files to the hard disk and restart the computer. You can remove the installation CD at this time. DO NOT choose to boot from the installation CD. Installation will continue after the computer restarts from the hard disk.
9. The **Regional and Language Options** screen opens. When prompted with the default regional and language selections, verify that they are correct and then click Next to continue without making any changes.
10. The **Personalize Your Software** screen appears. Type your name and the name **Busicorp** as the organizational name and click Next to continue.

11. The **Your Product Key** screen opens. Enter the product key value for this copy of Windows XP Professional and click Next to continue. If you using an evaluation copy, you will not be prompted for the product key.
12. The **Licensing Modes** screen appears (Figure 1-3). Click Next to accept the default license mode (per server licensing) and continue.



Setup will complete approximately: 33 minutes

Windows Setup

Licensing Modes
Windows Server 2003 supports two licensing modes.

Select the licensing mode you want to use.

● Per server. Number of concurrent connections: 5
Each connection must have its own Client Access License.

○ Per Device or Per User.
Each device or user must have its own Client Access License.

To avoid violation of the License Agreement, use Licensing (which is located in Administrative Tools) to record the number of Client Access Licenses purchased.

**Figure 1-3: Windows Server 2003 Setup/Licensing Modes**

13. The **Computer Name and Administrator Password** screen opens. Unless provided with an alternate computer name by your instructor or network administrator, enter the following information and then click Next to continue.

    Computer name: **Server1**
14. What happens?

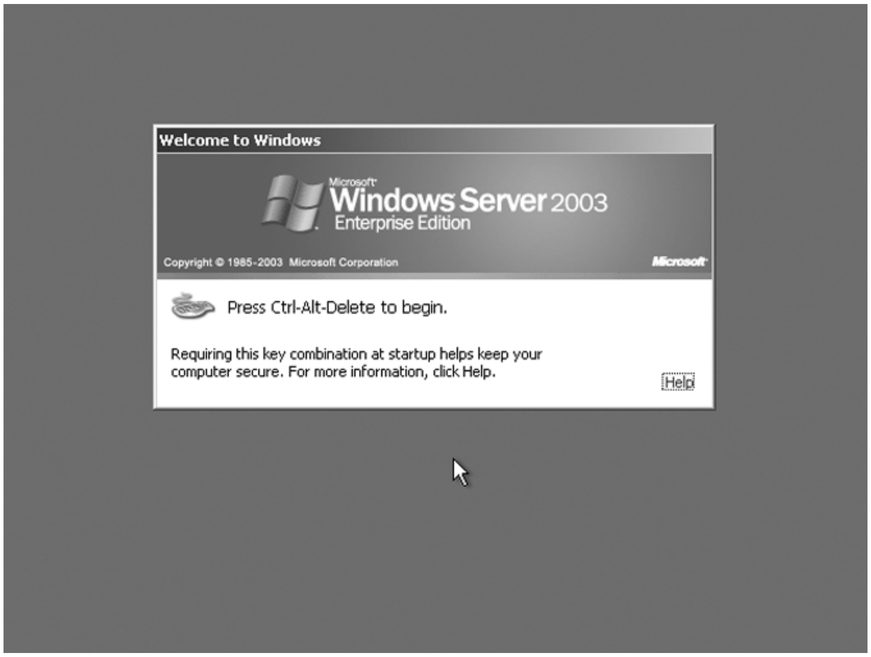
    ______________________________________________________________

    ______________________________________________________________
15. Click No.
16. Type and confirm the password **pass** and click **Next**.
17. What happens?

    ______________________________________________________________

    ______________________________________________________________
18. Click No.
19. Type **P&ssword** as the password and click Next.

20. If a modem is detected, the **Modem Dialing Information** screen opens. Enter the necessary information including the area code or city code, if necessary, and then click Next. This screen is omitted if the computer does not have a modem
21. The **Date and Time Settings** screen opens. Select your local time zone and click Next to continue. There will be a delay while the computer prepares to install networking.
22. The **Networking Settings** screen opens. When prompted for network settings, keep the default **Typical Settings** and click Next.
23. The **Workgroup or Computer Domain** screen opens. Keep the default workgroup name and click Next to continue.
24. The computer will restart automatically when setup is complete and the **Welcome to Microsoft Windows Server 2003** initial logon screen will appear (Figure 1-4).


Welcome to Windows
Microsoft Windows Server 2003
Enterprise Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft
Help

Press Ctrl-Alt-Delete to begin.

Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

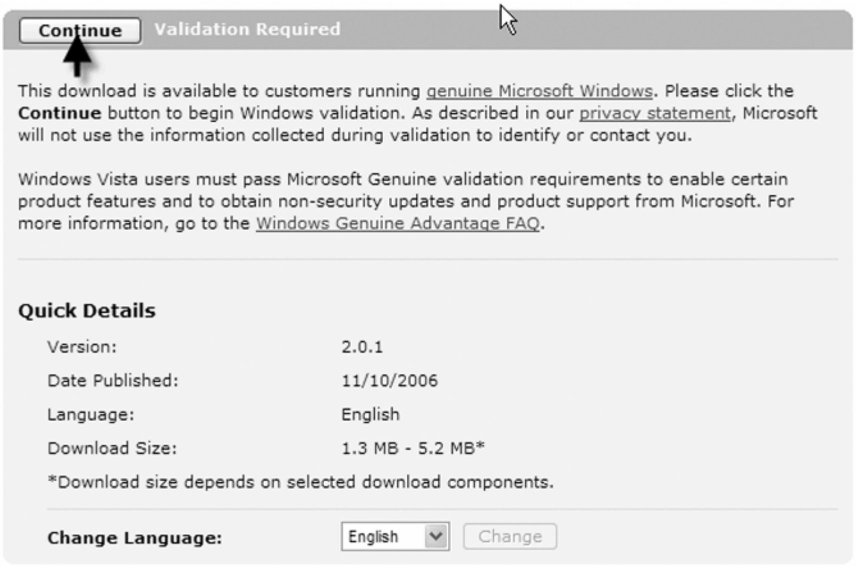
**Figure 1-4: Welcome to Windows Server 2003**

25. Press Ctrl + Alt + Del to open the **Log on to Windows** dialog box.
26. Type **P&ssword** as the password and click OK.

| Project 1.4 | Using Microsoft Security Baseline Analyzer |
|---|---|
| Overview | Microsoft Security Baseline Analyzer (MBSA) is a vulnerabilities scanner that can be downloaded from Microsoft's website. You can use it to scan one or more computers for vulnerabilities.<br>Microsoft frequently releases security updates to correct vulnerabilities as they are discovered. One important way to secure computers is to ensure that they are kept up-to-date. |
| Outcomes | After completing this project, you will know how to:<br>▲ use MSBA to scan a computer for vulnerabilities<br>▲ install service packs and security updates |
| What you'll need | To complete this project, you will need:<br>▲ a computer running Windows XP Professional<br>▲ access to the Internet |
| Completion time | 90 minutes, depending on Internet connection speed |
| Precautions | In Step 9, you may be prompted to install the Genuine Microsoft Validation Tool ActiveX control. If prompted, install this control. You must validate your copy of Windows before you can continue, so this is required.<br>If the computer is part of an existing network, you must review the project steps with your network administrator. Your network administrator may need to make changes to the project steps. |

## ■ PART A: Download and install MBSA

1. Launch **Internet Explorer**.
2. Type www.microsoft.com in the **Address** bar and click Go.
3. Type **mbsa** in the **Search** field and click Search.
4. If you are prompted about sending information to the Internet, click Yes.
5. If you are prompted about turning on **AutoComplete**, click Yes.
6. Click the link for **Microsoft Baseline Security Analyzer 2.0**.
7. Click **Download Now**.
8. Click **English**.
9. Click Continue to validate that you are running a genuine version of Windows XP, as shown in Figure 1-5.



This download is available to customers running genuine Microsoft Windows. Please click the **Continue** button to begin Windows validation. As described in our privacy statement, Microsoft will not use the information collected during validation to identify or contact you.

Windows Vista users must pass Microsoft Genuine validation requirements to enable certain product features and to obtain non-security updates and product support from Microsoft. For more information, go to the Windows Genuine Advantage FAQ.

**Quick Details**

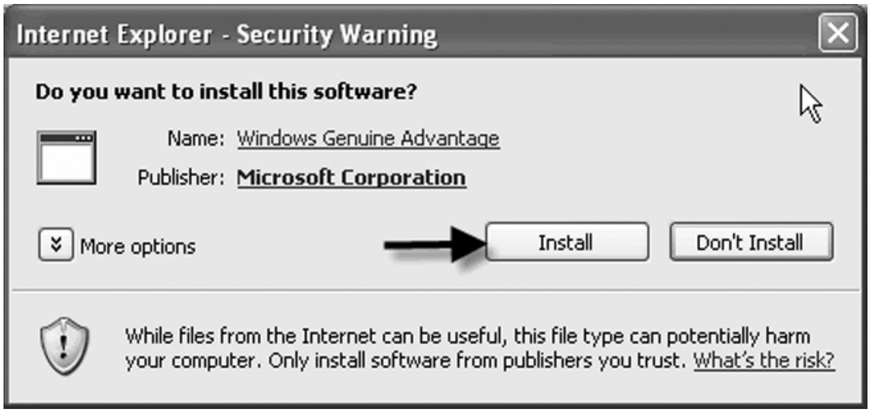
| | |
|---|---|
| Version: | 2.0.1 |
| Date Published: | 11/10/2006 |
| Language: | English |
| Download Size: | 1.3 MB - 5.2 MB* |

*Download size depends on selected download components.

**Change Language:** English

Figure 1-5: Validating Windows

10. When prompted to install and run **Windows Genuine Advantage**, click Install (Figure 1-6).



Internet Explorer - Security Warning

**Do you want to install this software?**

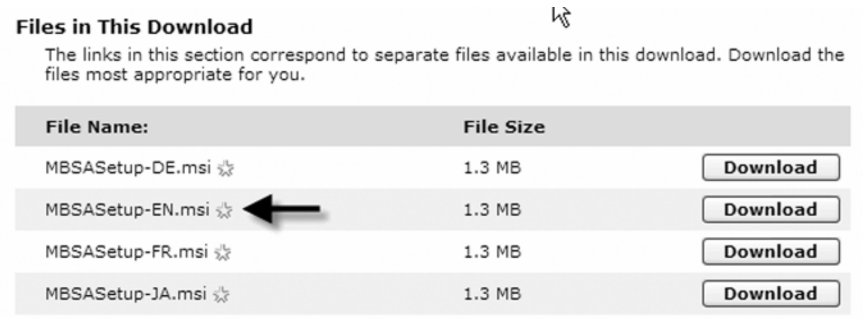
Name: Windows Genuine Advantage

Publisher: **Microsoft Corporation**

While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

Figure 1-6: Installing Windows Genuine Advantage

11. After installation completes, scroll down and locate the **Files in This Download** section.
12. Click the Download button associated with **MBSASetup-EN.msi**, as shown in Figure 1-7.



**Files in This Download**

The links in this section correspond to separate files available in this download. Download the files most appropriate for you.

| File Name: | File Size | |
|---|---|---|
| MBSASetup-DE.msi | 1.3 MB | Download |
| MBSASetup-EN.msi | 1.3 MB | Download |
| MBSASetup-FR.msi | 1.3 MB | Download |
| MBSASetup-JA.msi | 1.3 MB | Download |

**Figure 1-7: Selecting the file to download**

13. Read the warning and click Save.
14. Create a folder on your **C:** drive named **mbsa**. Open that folder and click Save.
15. The download time will depend on the speed of your connection. After it completes, click Run. When prompted whether to run the file, click Run again.
16. When the **Welcome** screen appears, click Next.
17. Click **I accept the license agreement** and click Next.
18. Accept the default location and click Next.
19. Click Install.
20. Click OK.
21. Close the browser.

## ■ PART B: Run MSBA

1. Open the **Start** menu, point to **All Programs**, and then select **Microsoft Baseline Security Analyzer 2.01**.
2. Click **Scan a computer**.
3. Keep the default settings and click **Start scan**.
4. MBSA will download updates from Microsoft's website. Why is it important to download updates before beginning the scan?

    ______________________________________________________________________

    ______________________________________________________________________

5. MBSA will scan the computer.
6. Review the settings. What is the worst problem detected?

    ______________________________________________________________________

    ______________________________________________________________________

7. Was a complete scan run?

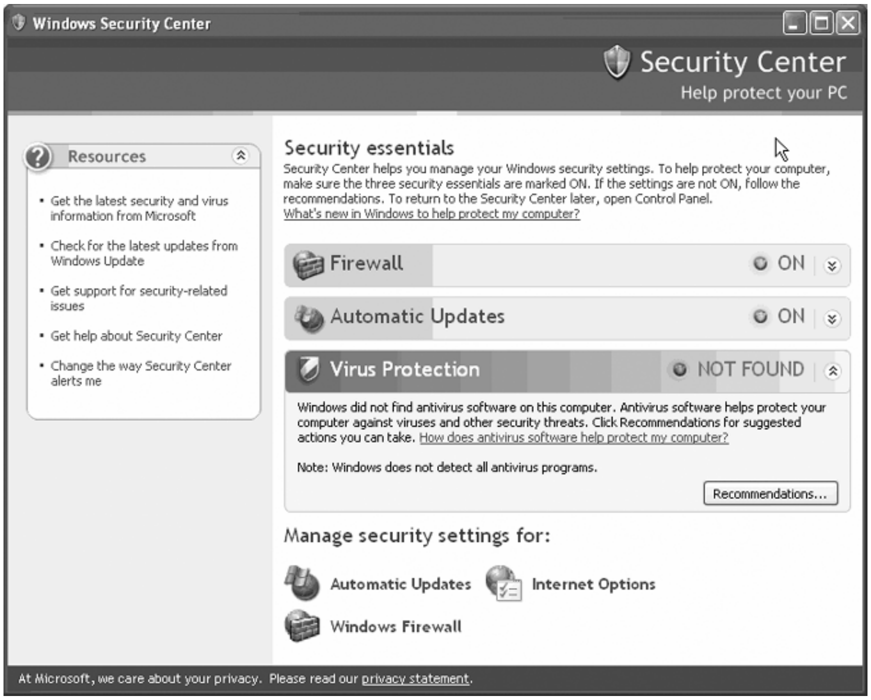
    ______________________________________________________________________

    ______________________________________________________________________

8. Click **How to correct this** under **Scanning Requirements**.

## ■ PART C: Install Service Pack 2 on a Windows XP computer

1. Under **Windows Security Updates**, click **Result Details**.
2. Scroll down to the bottom and click **Download** in the **Windows XP Service Pack 2** row.
3. Read the security warning and click Open.
4. **Service Pack 2** will download. This process will take an hour or more, depending on your connection speed. After it has downloaded, click Next.
5. Click I Agree.
6. Click Next.
7. Click Next to accept the default location for the uninstall files.
8. The **Setup Wizard** will backup your current operating system files, and then install Service Pack 2.
9. Click Finish. Your computer will be restarted.
10. Click **Help protect my PC by turning on Automatic Updates now**.
11. Click Next.
12. One of the features installed by Service Pack 2 is **Windows Security Center**, shown in Figure 1-8. It allows you to enable, disable, and manage settings for **Windows Firewall** and **Automatic Updates**. It also allows you to manage Internet options. If you have virus protection software on your computer, it allows you to enable that also.



- Get the latest security and virus information from Microsoft
- Check for the latest updates from Windows Update
- Get support for security-related issues
- Get help about Security Center
- Change the way Security Center alerts me

Security essentials

Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.
What's new in Windows to help protect my computer?

Windows did not find antivirus software on this computer. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?

Note: Windows does not detect all antivirus programs.

At Microsoft, we care about your privacy. Please read our privacy statement.

**Figure 1-8: Windows Security Center**

## PART D: Install updates on a Windows XP computer

1. Click **Check for the latest updates from Windows Update**.
2. Click **Express**.
3. Click **Download and Install Now**.
4. Click **Restart Now**. After **Internet Explorer 7.0** is installed, you will be prompted whether to install the automatic **Phishing Filter**. For now, select **Ask me later** and click **OK**.
5. Repeat Steps 1–4 until all updates have been installed.
6. When you attempt to check for the latest updates and 0 updates are returned, click **Review your update history** in the left-hand pane.
7. Scroll through the updates. If any appear with a red **X**, click them to install them manually, and then restart the computer if prompted.

## ■ PART E: Scan the computer again

1. Open the **Start** menu, point to **All Programs** and select **Microsoft Baseline Security Analyzer 2.01**.
2. Click **Scan a computer**.
3. Keep the default settings and click **Start scan**.
4. What are the results this time?

____________________________________________________________

____________________________________________________________

| **Project 1.5** | **Viewing Local Security Policy** |
|---|---|
| Overview | Windows XP Professional includes Local Security Policy, which allows you to configure an automated security policy. In this project, you will familiarize yourself with the settings available through Local Security Policy. |
| Outcomes | After completing this project, you will know how to:<br>▲ view Local Security Policy settings |
| What you'll need | To complete this project, you will need:<br>▲ to have completed Project 2.4 |
| Completion time | 15 minutes |
| Precautions | Do not make changes to Local Security Policy. The purpose of this activity is to familiarize you with the configuration settings that can be enforced through Local Security Policy. |

## ■ PART A: View Account Policies

1. Open the **Start** menu and select **Control Panel**.
2. Select **Performance and Maintenance**, and then select **Administrative Tools**.
3. Double-click **Local Security Policy** (Figure 1-9).

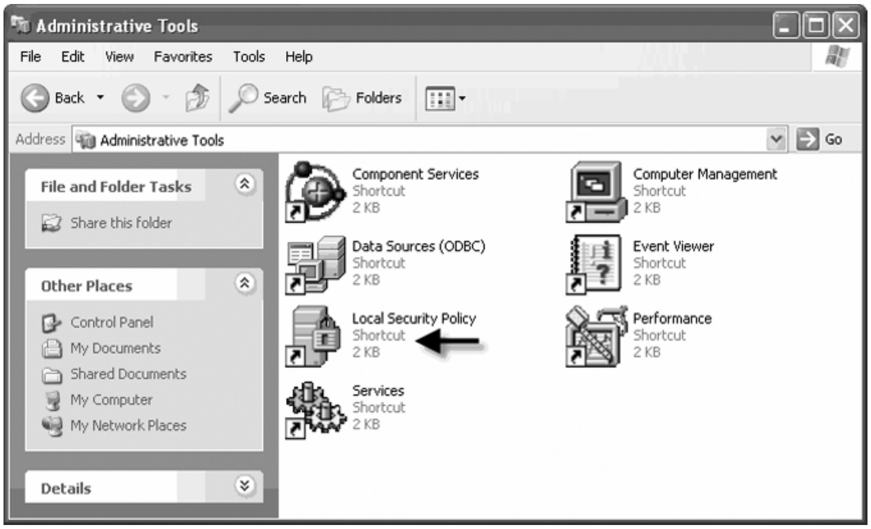


**Figure 1-9: Launching Local Security Policy**

4. What categories are listed?

______________________________________________________________

______________________________________________________________

5. Expand **Account Policies** (Figure 1-10).

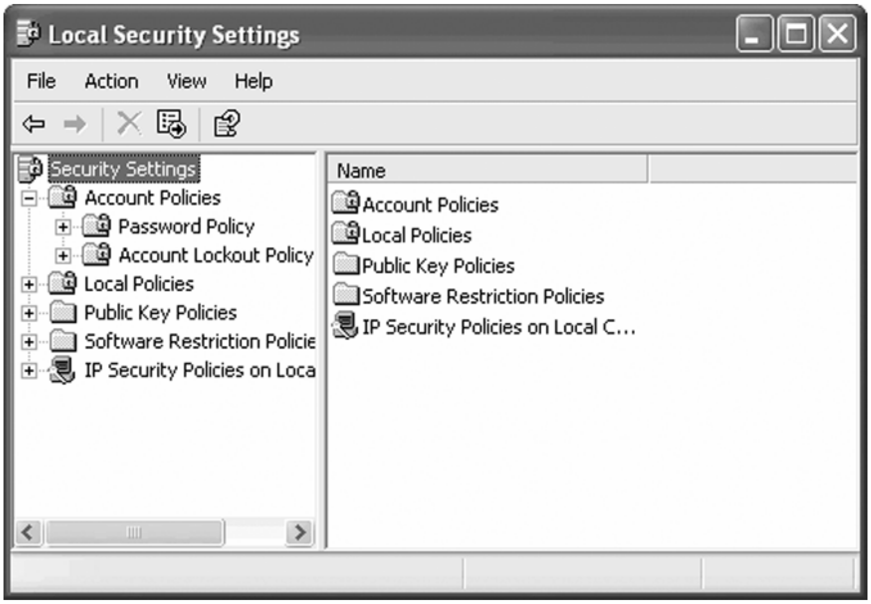
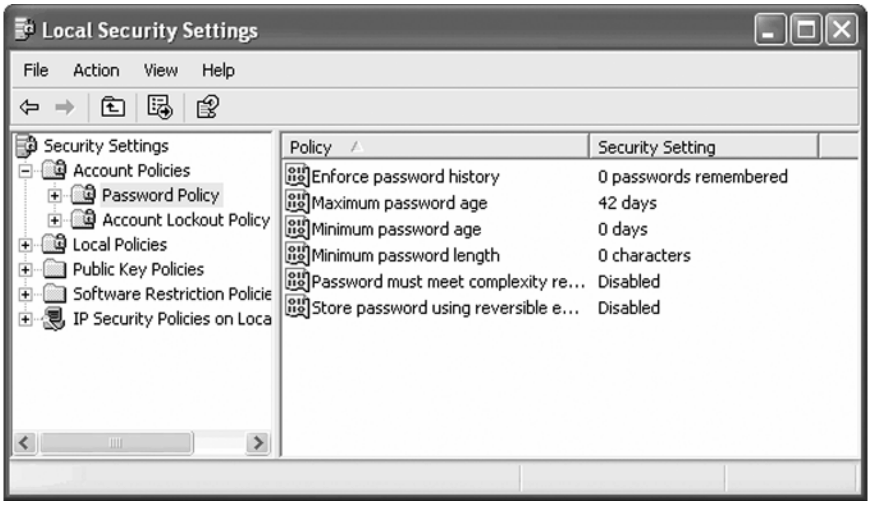


**Figure 1-10: Account Policies node**

6. What policies are listed?

7. Select **Password Policy** in the left-hand pane (Figure 1-11).



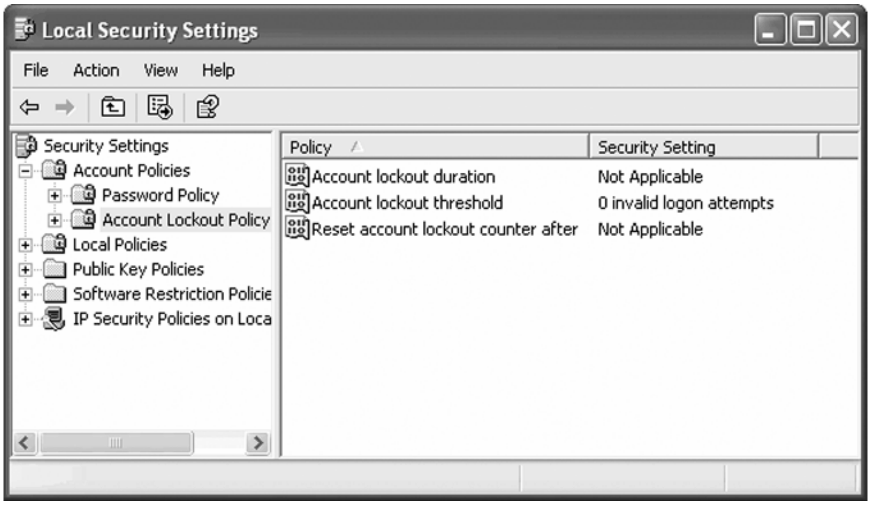
| Policy | Security Setting |
|---|---|
| Enforce password history | 0 passwords remembered |
| Maximum password age | 42 days |
| Minimum password age | 0 days |
| Minimum password length | 0 characters |
| Password must meet complexity re… | Disabled |
| Store password using reversible e… | Disabled |

**Figure 1-11: Password Policy node**

8. Review the policy settings. What two types of attacks can you mitigate using the **Password must meet complexity requirements** setting?

9. How does forcing users to change their password help mitigate a social engineering attack?

10. Select **Account Lockout Policy** (Figure 1-12).



| Policy | Security Setting |
|---|---|
| Account lockout duration | Not Applicable |
| Account lockout threshold | 0 invalid logon attempts |
| Reset account lockout counter after | Not Applicable |

**Figure 1-12: Account Lockout Policy node**

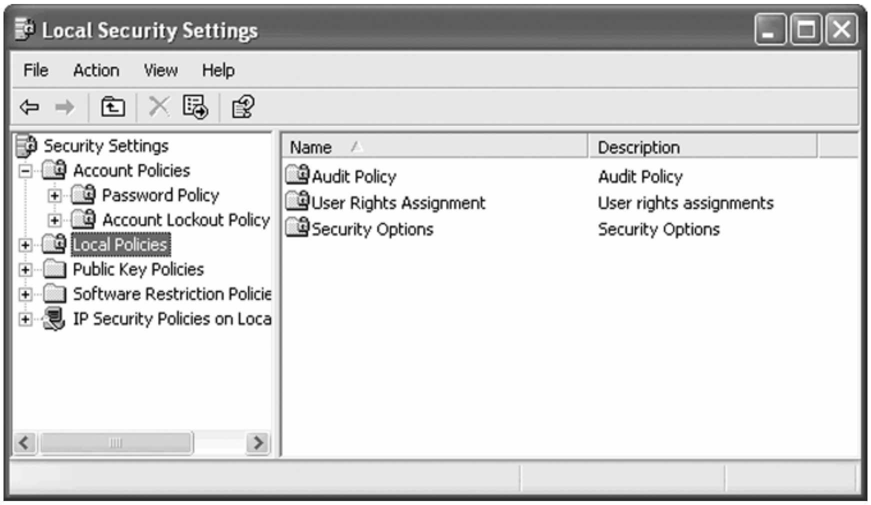
11. Review the policies. How might setting an **Account Lockout Policy** lead to a denial of service attack?

____________________________________________________________

____________________________________________________________

## ■ PART B: View Local Policies

1. Select **Local Policies** (Figure 1-13).



| Name | Description |
|---|---|
| Audit Policy | Audit Policy |
| User Rights Assignment | User rights assignments |
| Security Options | Security Options |

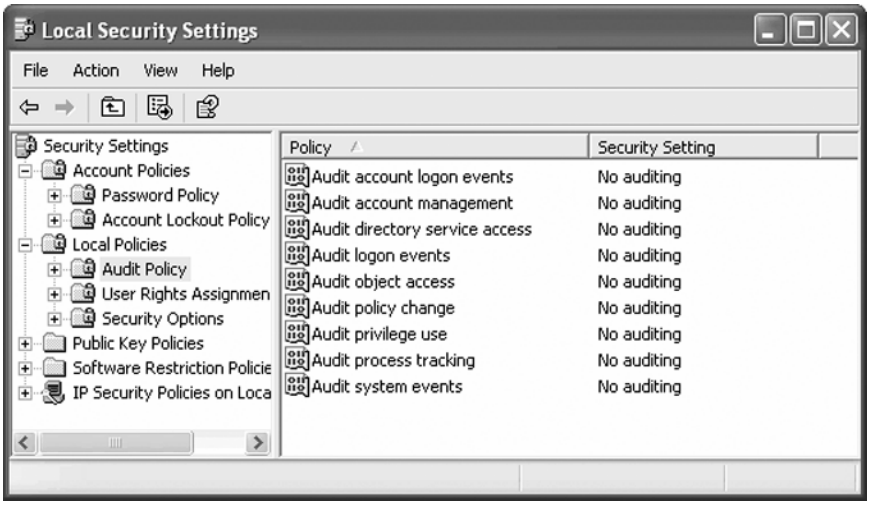
**Figure 1-13: Local Policies node**

2. What options are available?

______________________________________________________________

______________________________________________________________

3. Double-click **Audit Policy** (Figure 1-14).



| Policy | Security Setting |
|---|---|
| Audit account logon events | No auditing |
| Audit account management | No auditing |
| Audit directory service access | No auditing |
| Audit logon events | No auditing |
| Audit object access | No auditing |
| Audit policy change | No auditing |
| Audit privilege use | No auditing |
| Audit process tracking | No auditing |
| Audit system events | No auditing |

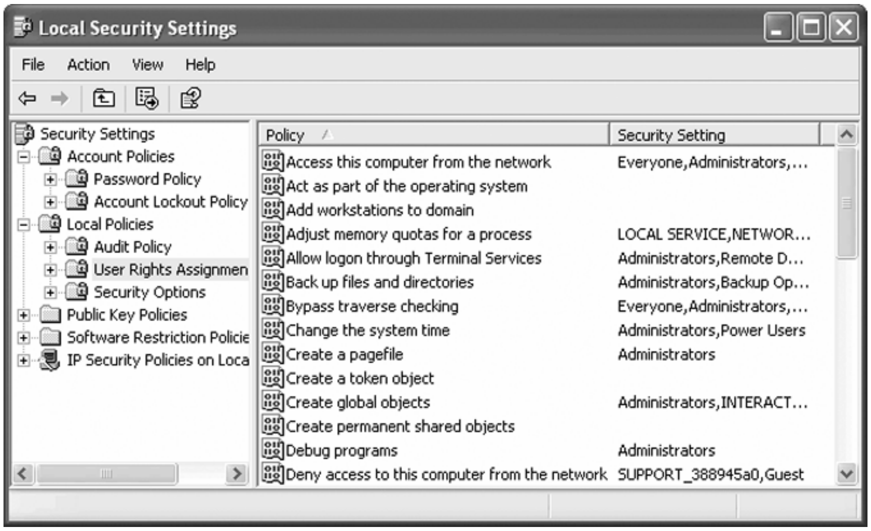
**Figure 1-14: Audit Policy node**

4. What types of auditing is performed by default?

______________________________________________________________

______________________________________________________________

5. Select **User Rights Assignment** (Figure 1-15).



| Policy | Security Setting |
|---|---|
| Access this computer from the network | Everyone,Administrators,... |
| Act as part of the operating system | |
| Add workstations to domain | |
| Adjust memory quotas for a process | LOCAL SERVICE,NETWOR... |
| Allow logon through Terminal Services | Administrators,Remote D... |
| Back up files and directories | Administrators,Backup Op... |
| Bypass traverse checking | Everyone,Administrators,... |
| Change the system time | Administrators,Power Users |
| Create a pagefile | Administrators |
| Create a token object | |
| Create global objects | Administrators,INTERACT... |
| Create permanent shared objects | |
| Debug programs | Administrators |
| Deny access to this computer from the network | SUPPORT_388945a0,Guest |

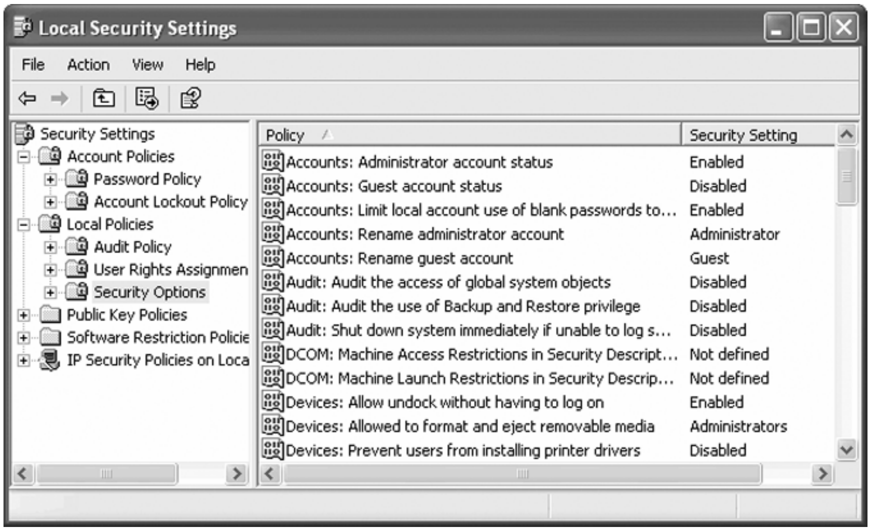
**Figure 1-15: User Rights Assignment node**

6. What users are allowed to access this computer from the network?

7. How could you reduce the likelihood of an attack over the network?

8. What additional accounts are allowed the **Log on locally** right?

9. Click **Security Options** (Figure 1-16).



| Policy | Security Setting |
|---|---|
| Accounts: Administrator account status | Enabled |
| Accounts: Guest account status | Disabled |
| Accounts: Limit local account use of blank passwords to... | Enabled |
| Accounts: Rename administrator account | Administrator |
| Accounts: Rename guest account | Guest |
| Audit: Audit the access of global system objects | Disabled |
| Audit: Audit the use of Backup and Restore privilege | Disabled |
| Audit: Shut down system immediately if unable to log s... | Disabled |
| DCOM: Machine Access Restrictions in Security Descript... | Not defined |
| DCOM: Machine Launch Restrictions in Security Descrip... | Not defined |
| Devices: Allow undock without having to log on | Enabled |
| Devices: Allowed to format and eject removable media | Administrators |
| Devices: Prevent users from installing printer drivers | Disabled |

**Figure 1-16: Security Options node**

10. Why might you want to change the name of the **Administrator** account?

11. Close **Local Security Policy**.

| Project 1.6 | Creating a Written Security Policy |
|---|---|
| Overview | A written security policy provides guidelines for the employees of a company to follow when making decisions about the security design and implementation. It also provides a recovery plan if a security breach occurs. |
| Outcomes | After completing this project, you will know how to:<br>▲ identify the types of information that should be included in a written security plan |
| What you'll need | To complete this project, you will need:<br>▲ the worksheet below |
| Completion time | 30 minutes |
| Precautions | None |

## Scenario

Busicorp does not currently have a security policy in place. You have been asked to work with others to draft a written security policy for Busicorp. The policies should be designed to mitigate the risks to Busicorp's assets. Use the scenario provided in Project 1.1.

## ■ PART A: Define a physical security policy

1. Your risk analysis identified at least two areas where physical security needs to be improved. Define a security policy that will help mitigate the risk of physical access to resources.

______________________________________________________________

______________________________________________________________

______________________________________________________________

## ■ PART B: Define a personnel security policy

1. What new hire policy will help prevent a social engineering attack?

______________________________________________________________

______________________________________________________________

2. Identify the steps that should be taken when an employee leaves the company voluntarily.

________________________________________________________

________________________________________________________

3. Identify any additional steps that should be taken when an employee is terminated.

________________________________________________________

________________________________________________________

## ■ PART C: Define an operations management policy

1. Identify some policies that should guide the day-to-day tasks of IT personnel.

________________________________________________________

________________________________________________________

________________________________________________________

## ■ PART D: Define an access control policy

1. Identify the types of data stored in the SQL Server database and who should be allowed to access it in Table 1-4.

**Table 1-4: Identifying Data Types and Access Permissions**

| Type of data | Who should access |
|---|---|
| | |
| | |
| | |

## ■ PART E: Define an systems development and maintenance policy

1. Which computers should be subject to systems development and maintenance policies?

________________________________________________________

________________________________________________________

## ■ PART F: Define a business continuity planning policy

1. Identify the data that should be regularly backed up.

______________________________________________________________

______________________________________________________________

______________________________________________________________

2. Which two resources are most important to protect with a redundant server?

______________________________________________________________

______________________________________________________________

______________________________________________________________