SECTION 24 (Self-Study) Identify How to Protect Your Network Against Viruses

The following objective will be tested:

- Describe What You Can Do to Prevent a Virus Attack

In this section you learn about viruses and how you can protect network data and resources from a virus attack.

Objectives

1. Identify Types of Viruses
2. Identify What You Can Do to Prevent a Virus Attack
3. Identify How to Recognize and Remove a Virus

Introduction

Computer viruses are data destructive programs that spread destruction to other computers and programs. Every year, thousands of people and companies suffer often-irrecoverable damage to their systems and data.

A computer virus can only survive, attack, and propagate in computer memory. Computer memory is usually the RAM and disk storage such as the hard disk and disk drives.

To prevent or handle a virus attack, you need to know how viruses enter your computer system, how they infect your system, and how they eventually spread and cause more damage.

In this section, you learn about types of viruses and the characteristics of a virus attack. You also identify the entry points of a virus, learn guidelines to prevent a virus attack, and identify how to remove a virus in the event of a virus attack.

Objective 1 Identify Types of Viruses

Although the term virus is often used to describe any software that attacks a web service or server, there are actually 3 basic types of programmed threats that can violate network security:

- **Virus.** A code fragment (not an independent program) that reproduces by attaching to another program.

  A virus can damage data directly or degrade system performance by taking over system resources, which are then not available to authorized users.

  Viruses are classified according to how they infect the computer system. They include the following categories:

  - **Boot sector viruses.** These are usually transmitted when an infected disk is left in the drive and the system is rebooted.

    The virus is read from the infected boot sector of the disk and written to the master boot block. As soon as you restart your computer, the virus is triggered from the boot block and can cause serious consequences.

    For example, the CIH/Chernobyl virus overwrites the first 2048 sectors of the hard drive with random data. This area contains important information about the files on the computer.

    Without this file information, the computer assumes that the hard drive is empty and will not run the operating system.

- **Program or file viruses.** These are pieces of code that attach themselves to executable programs or files. Once the infected program is run or the file is opened, the virus is transferred to the computer’s memory and may replicate itself further.

  For example, a MIME header for a web page tells your web browser what types of files are included (embedded) in the page (such as graphics or sound files).

  If an EXE file written by an attacker represents itself as a JPEG file in the MIME header, the web browser will evaluate the file as safe and let it pass through.

  When the file is opened and run as an EXE file on your computer, it can cause significant harm to your computer and other computers on the network (depending on your network rights and access privileges).

- **Macro viruses.** These are the most common viruses. They infect files run by applications that use macro languages, like Microsoft Word or Excel.

  The virus looks like a macro in the file. When the file is opened, the virus can execute commands understood by the application's macro language.

- **Multipartite viruses.** These have characteristics of both boot sector viruses and file viruses. They may start out in the boot sector and spread to applications, or vice versa.

- **Worm.** An independent program that reproduces by copying itself from one system to another, usually over a network.

  Like a virus, a worm can damage data directly, or it can degrade system performance by consuming system resources and even shutting down a network.

- **Trojan horse.** An independent program that appears to perform a useful function but that hides another unauthorized program inside it.

When an authorized user tries to perform a task with the program, the Trojan horse performs the unauthorized function as well.

Although you can configure computers to take countermeasures against these threats, viruses generally rely on a person's actions (such as opening an email attachment) to spread the infection.

This means that a key factor in protecting against most viruses, worms, and Trojan horses is to implement proper policies and train users to prevent viruses from being installed on their workstations.

The term *virus* is used throughout this section when referring to viruses, worms, and Trojan horses.

Objective 2 Identify What You Can Do to Prevent a Virus Attack

The best cure for any virus is prevention. Viruses infect and damage unsuspecting computers, so it is vital to take preventive steps. To avoid virus infection, you need to do the following:

- Develop a Virus Protection Plan
- Install Antivirus and Data Integrity Software
- Scan, Update, and Upgrade Automatically
- Back Up Your Data Regularly
- Consider Every Disk, Program, and Email Attachment as a Threat
- Use Caution when You Download Files from the Internet
- Be Aware of Virus Hoaxes
- Educate Your Users

Develop a Virus Protection Plan

Viruses can infect and cause irreparable damage to your computers. It is vital to take steps to prevent viruses. These steps need to be organized and recorded in a virus prevention plan or strategy.

Make sure you do the following in your virus protection plan:

- Identify the Entry Points for Viruses
- Specify Responsibilities and Authority
- Describe the Installation and Use of Antivirus Tools

Identify the Entry Points for Viruses

To define a virus prevention plan, you need to first identify all entry points in your network through which a virus can attack.

All viruses enter the network through 1 of the following entry points:

- **Disk drives.** Disks or CDs that you insert into these drives can be a possible source of virus infection.
- **External storage media.** Files stored in these media can be infected with a virus.
- **Infected documents.** Infected documents from applications such as Word and Excel that are used by multiple users on your network can also be a source of viruses.
- **SMTP gateways.** Email is a major source of spreading viruses. Virus-infected files can be sent as email attachments that are often program files or Word documents containing macros.

  These viruses rapidly spread across your network through internal mailing systems.

- **Internet gateways.** Files downloaded from web sites, FTP sites, and USEnet groups can be infected with viruses that infect a computer and subsequently an entire network.
- **Wireless Internet devices.** Wireless devices (such mobile phones, PDAs, and laptops with wireless cards) that do not have a virus prevention system of their own can also propagate viruses.

Specify Responsibilities and Authority

Your virus protection plan should specify how much responsibility and authority users and network administrators have to take specific actions that protect their computers against viruses and similar programmed threats.

For example, you may decide that all employees need to be responsible for updating the antivirus software on their computers, but the network administrator needs to be responsible for making the latest version of the software available to employees from the company internal web portal.

Describe the Installation and Use of Antivirus Tools

Your plan should describe how to use installed antivirus tools for workstations and explain any user limitations on downloading and installing new software.

Install Antivirus and Data Integrity Software

Antivirus software provides important tools for protecting your systems from computer viruses. You should install antivirus software on all computers in your network.

Most antivirus programs allow users to completely scan all files read from disk drives or downloaded from the intranet/Internet.

Data integrity tools help you detect if files have been modified on a system. Some integrity checkers can help you identify the virus that modified a file, but others might only be able to alert you to the changes.

Integrity checkers are useful for detecting a possible infection and for helping to detect intruders.

For a list of antivirus software and data integrity checker vendors, see http://www.cert.org/other_sources/viruses.html#VI on the CERT web site.

Scan, Update, and Upgrade Automatically

After you install the antivirus software, you should use it to scan files on your system.

Many antivirus software programs give you the option of selecting the time when you want your antivirus software to scan your system.

You can configure the software to start scanning when you switch on your system, or start scanning when the system is not being used.

New strains of viruses are created and spread daily. Therefore, you need to have the updated versions of definition files on your system. Definition files are provided by antivirus software vendors and are used by the antivirus software to identify a virus.

If you do not have updated definition files, new virus programs can infect your antivirus software and infect all files that the software is scanning.

You can configure your antivirus software to look for updated versions of the definition files on your antivirus vendor's site. When a new version of a definition file is detected, your antivirus software can automatically download the file on your system.

Back Up Your Data Regularly

Although you might have several virus prevention plans in place, you can never completely secure your network (especially internally).

Backing up your data regularly is an effective method of preventing data loss because of a virus attack. In addition to a local backup device (such as a tape drive), secure services are available on the Internet for backing up your network data.

Consider Every Disk, Program, and Email Attachment as a Threat

You should always consider every disk, program, and email attachment as a threat. Never assume that files that have been sent by friends, family, business associates, or other employees are not infected.

When handling files received from others on removable media (such as disks) or through email, follow these guidelines:

- Write-protect any data source disk before inserting it into the drive.
- Scan the files on your disks before copying them to your computer.
- Change your computer's CMOS boot sequence to start with drive C first and then drive A. This prevents the computer from attempting to boot from an infected disk left in the drive.

- Scan your programs before executing them on computers that contain critical data.
- Do not download attachments or files that you have received from strangers.
- If you need to open an attached file, download it to a disk, and then scan it with your antivirus software before executing or opening the file.

Use Caution when You Download Files from the Internet

You should use caution when you download files from the Internet. Download files directly to a quarantined scanning area, whenever possible.

You might consider dedicating a computer to testing all new files and disks. All files on the control machine can then be systematically scanned for viruses before you access them.

Be Aware of Virus Hoaxes

You need to be careful about virus hoaxes on the Internet. If you receive a virus warning, check your antivirus software provider's web site to make sure the warning is accurate.

For example, many ignored the Love Bug virus warnings because of the number of virus hoaxes circulating on the Internet at the time. By ignoring a valid warning, many companies lost thousands of dollars when the Love Bug invaded their networks.

Web sites such as www.cert.org and www.symantec.com track current viruses and provide the latest information on virus hoaxes.

Educate Your Users

Educating users about antivirus procedures is the most critical and effective measure you can take to prevent network virus attacks. Any prevention plan or antivirus software is ineffective without actual user participation.

As part of your employee awareness strategy, make sure you do the following:

- Emphasize the risks to the network if even 1 computer does not have antivirus software installed.
- Make sure employees who work on computers at home follow the same antivirus procedures they use at office, whether on personal or company-supplied computers.
- Make sure disks brought from home by employees are write-protected and scanned before being used on the network.

Objective 3 Identify How to Recognize and Remove a Virus

Although you may take precautions to prevent a virus attack, there is still a chance that a sophisticated virus or unaware employee can result in a virus attack.

To recognize and remove a virus, you should do the following:

- List the Symptoms of an Infected Computer
- List the Steps for Removing a Virus

List the Symptoms of an Infected Computer

The following are common symptoms of a computer infected with a virus:

- The computer fails to start.
- Programs will not launch or they fail when simple commands are performed.
- Filenames change or become unreadable.
- File contents change or are no longer accessible.
- Unusual words or graphics appear on the screen.
- Hard drives or disks are reformatted.
- Variations occur in computer performance, such as slowdowns in loading or operation.

It is important for you to be aware of these symptoms and make sure your employees are educated in observing and reporting them.

List the Steps for Removing a Virus

If you detect a virus at your site, do the following to contain and eliminate the virus:

1. Determine the type of virus and the severity of the infection.

   This information is important for the cleanup phase.

2. Isolate all infected systems and disks.

   This helps to contain further spread of the virus.

3. Make sure you have a clean disk formatted as a system disk.

   The system disk should be formatted using the FORMAT A: /S command. Copy the antiviral programs on this or another clean disk and write-protect these disks.

4. Use the clean system disk to boot up all systems with suspected infection.

   This ensures that no virus that could affect the scanning program code is present in memory.

5. Scan every physical and logical hard disk, as well as every disk.

   This avoids reinfection at a later date.

6. Back up the necessary data and executable files to trusted, clean media.

   If you are concerned that an executable file on a server, workstation, or disk is infected, exclude that file from the backup.

7. Clean the infected standalone workstations.

   When the virus is a common boot sector virus, the cleanup is usually not too difficult and can normally be handled by any commercial antivirus product.

   However, file-infecting viruses might create problems as they become part of the file. Removing the virus from the file using an antivirus cleaning program can corrupt the original executable file.

   If clean copies of all executable files exist, delete all infected programs for a small number of infections, or reformat the disk if most files are infected, and then reload clean copies of the executables.

8. Scan the data files on the server.

   Use an antivirus program to scan the data files on the server for any viruses. Run the program from a trusted source such as a clean CD or disk.

9. Clean the disk.

   After you clean the workstations and the server, clean infected disks to avoid a repeat attack.

Locate and clean all infected disks that might have been used on the workstation. The easiest method of cleaning the disks is to copy all uninfected files to a clean disk, using a clean system, and then reformat the disk.

By following these general steps, you can eliminate most viruses from your network system.

Exercise 24-1 Test Your Understanding

10 minutes

Answer the following:

1. An employee has reported that her Word documents have not been formatting properly. You ask if she's recently opened an email from an unknown source with an attached Word document called LIST.DOC. Which of the following types of viruses do you suspect is causing problems?

a. File virus

b. Macro virus

c. Encrypted virus

d. Polymorphic virus

2. You accidentally turn on a lab computer with a disk in drive A. You do not know who left the disk in the drive or where it came from. Now the computer takes much longer to complete even simple tasks. Which of the following types of viruses do you suspect is causing problems?

a. File virus

b. Encrypted virus

c. Polymorphic virus

d. Boot virus

e. Logic bomb

3. As part of your virus protection plan, you want to include an intranet list of common symptoms employees can use to determine if their computers are infected with a virus. Which of the following should you include? (Choose 3.)

a. The computer begins to speed up its processing time.

b. Filenames change or become unreadable.

c. Files are listed by file size instead of name.

d. Unusual words or graphics appear on the screen.

e. File contents change or are no longer accessible.

f. Email messages arrive from unknown sources.

4. Which of the following are entry points for a virus? (Choose 3.)

a. External storage media

b. Email with text files as attachments

c. SMTP gateways

d. Wireless Internet devices

e. External printing devices

5. In addition to installing an antivirus program to protect your systems from computer viruses, what other type of tool can you install to help detect viruses?

a. Data integrity checker

b. Virus integrity checker

c. File quarantine eliminator

d. File integrity and quarantine checker

6. You receive an email attachment from an unknown or untrusted source, but you want to view the file. What is the best thing to do?

a. Download the file to your hard drive and then scan the file with your antivirus software before executing or opening the file.

b. Download the file to a server on your network, and then scan the file with your antivirus software before executing or opening the file.

c. Download the file to a disk (or burn it on a CD) and then scan the disk with your antivirus software before executing or opening the file.

d. Download a copy of the file to a disk and to your computer and then scan the disk with your antivirus software before executing or opening the copy on your hard drive.

e. Download a copy of the file to a disk and to a network server, scan the disk with your antivirus software, and then copy the file from the network server to your hard drive after you determine that the file is free from any virus.

7. Which of the following is the most effective measure you can take to prevent network virus attacks?

a. Install antivirus software.

b. Back up your data regularly.

c. Use caution when you download files from the Internet.

d. Be aware of virus hoaxes.

e. Educate your network users.

8. After detecting a virus on several employee workstations, you have determined the class of virus and used a clean system disk to boot all workstations with the suspected infection. What should you do next?

a. Back up the necessary data files to trusted, clean media.

b. Clean the infected workstations.

c. Scan every physical and logical hard disk on the workstations, as well as every disk the employees might have.

d. Check and clean any infected servers.

(End of Exercise)

Objectives Summary

In this section you learned about viruses and how you can protect network data and resources from a virus attack.

Objective 1 Identify Types of Viruses

Viruses include the following types:

- **Virus.** A code fragment (not an independent program) that reproduces by attaching to another program.

  A virus can damage data directly or degrade system performance by taking over system resources, which are then not available to authorized users.

  Viruses include the following categories:

  - Boot sector viruses
  - Program or file viruses
  - Macro viruses
  - Multipartite viruses

- **Worm.** An independent program that reproduces by copying itself from one system to another, usually over a network.
- **Trojan horse.** An independent program that appears to perform a useful function but that hides another unauthorized program inside it.

Although you can configure computers to take countermeasures against these threats, viruses generally rely upon people to spread the infection.

Objective 2 Identify What You Can Do to Prevent a Virus Attack

To avoid virus infection, you need to take the following preventative steps:

- **Develop a virus protection plan.** Make sure you identify the entry points for viruses, specify responsibilities and authority, and describe the installation and use of antivirus tools in your protection plan.
- **Install antivirus and data integrity software.** Install antivirus software on all computers in your network to scan files for viruses; install data integrity tools to detect if files have been modified.
- **Scan, update, and upgrade automatically.** Schedule antivirus software to scan files automatically and to prompt you to update the definition files for your software.
- **Back up your data regularly.** Backing up your data regularly with a device such as a tape drive is an effective method of preventing data loss because of a virus attack.
- **Consider every disk, program, and email attachment as a threat.** When handling files received from others on removable media (such as disks) or through email, follow procedures such as scanning the files and downloading the files to a disk for scanning before opening or executing them.
- **Use caution when you download files from the internet.** Download files directly to a quarantined scanning area or a computer dedicated to scanning files when possible.
- **Be aware of virus hoaxes.** Be careful about virus hoaxes on the Internet. If you receive a virus warning, check your software provider's web site to make sure the warning is accurate.
- **Educate your users.** Educating users about antivirus procedures is the most critical and effective measure you can take to prevent network virus attacks. Any prevention plan or antivirus software is ineffective without actual user participation.

Objective 3 Identify How to Recognize and Remove a Virus

To recognize and remove a virus, you should be able to do the following:

- **List the symptoms of an infected computer.** The following are common symptoms of a computer infected with a virus:
  - The computer fails to start.
  - Programs will not launch or they fail when simple commands are performed.
  - Filenames change or become unreadable.
  - File contents change or are no longer accessible.
  - Unusual words or graphics appear on the screen.
  - Hard drives or disks are formatted.
  - Variations occur in computer performance, such as slowdowns in loading or operation.
- **List the steps for removing a virus.** Follow these steps to contain and eliminate a virus:
  1. Determine the type of virus.
  2. Isolate all infected systems and disks.
  3. Make sure you have a clean disk formatted as a system disk.
  4. Use the clean system disk to boot all systems with suspected infection.
  5. Scan every physical and logical hard disk, as well as every disk.
  6. Back up the necessary data and executable files to trusted, clean media.
  7. Clean the infected standalone workstations
  8. Clean the infected server.
  9. Clean the disk.

Exercise Answers

Exercise 24-1 Test Your Understanding

1. An employee has reported that her Word documents have not been formatting properly. You ask if she's recently opened an email from an unknown source with an attached Word document called LIST.DOC. Which of the following types of viruses do you suspect is causing problems?

   b. Macro virus

2. You accidentally turn on a lab computer with a disk in drive A. You do not know who left the disk in the drive or where it came from. Now the computer takes much longer to complete even simple tasks. Which of the following types of viruses do you suspect is causing problems?

   d. Boot virus

3. As part of your virus protection plan, you want to include an intranet list of common symptoms employees can use to determine if their computers are infected with a virus. Which of the following should you include? (Choose 3.)

   b. Filenames change or become unreadable.

   d. Unusual words or graphics appear on the screen.

   e. File contents change or are no longer accessible.

4. Which of the following are entry points for a virus? (Choose 3.)

   a. External storage media

   c. SMTP gateways

   d. Wireless Internet devices

5. In addition to installing an antivirus program to protect your systems from computer viruses, what other type of tool can you install to help detect viruses?

a. Data integrity checker

6. You receive an email attachment from an unknown or untrusted source, but you want to view the file. What is the best thing to do?

c. Download the file to a disk (or burn it on a CD) and then scan the disk with your antivirus software before executing or opening the file.

7. Which of the following is the most effective measure you can take to prevent network virus attacks?

e. Educate your network users.

8. After detecting a virus on several employee workstations, you have determined the class of virus and used a clean system disk to boot all workstations with the suspected infection. What should you do next?

c. Scan every physical and logical hard disk on the workstations, as well as every disk the employees might have.