Network Vulnerabilities

by Sophia

WHAT'S COVERED

In this lesson, you will learn more about specific types of computer malware as well as threats to and vulnerabilities of data networks and computer systems.

Specifically, this lesson will cover the following:

1. Malware on the Network
    - 1a. Viruses
    - 1b. File Viruses
    - 1c. Macro Viruses
    - 1d. Boot-Sector Viruses
    - 1e. Multipartite Viruses
    - 1f. Ransomware
    - 1g. Logic Bomb
2. Exploits vs. Vulnerabilities
    - 2a. Zero-Day Exploits
    - 2b. Default Passwords/Settings
    - 2c. Unnecessary Running Services
    - 2d. Open Ports
    - 2e. Unpatched/Legacy Systems
    - 2f. Unencrypted Channels
    - 2g. Malicious Users
    - 2h. Trusted Users
    - 2i. Buffer Overflow
    - 2j. Wireless Threats
    - 2k. Backdoors
    - 2l. Network Reconnaissance

1. Malware on the Network

Malware (malicious software) is a term that describes any software that harms a computer, deletes data, or takes actions the user did not authorize. A wide array of malware types exists, including ones you have probably heard of, like viruses. Some types of malware require the assistance of a user to spread while others do not.

BIG IDEA

The prefix “mal” means bad, and “ware” is an abbreviation of software, so “malware” literally means bad software. There are many types of malware, but they all are harmful to your computer.

TERM TO KNOW

Malware

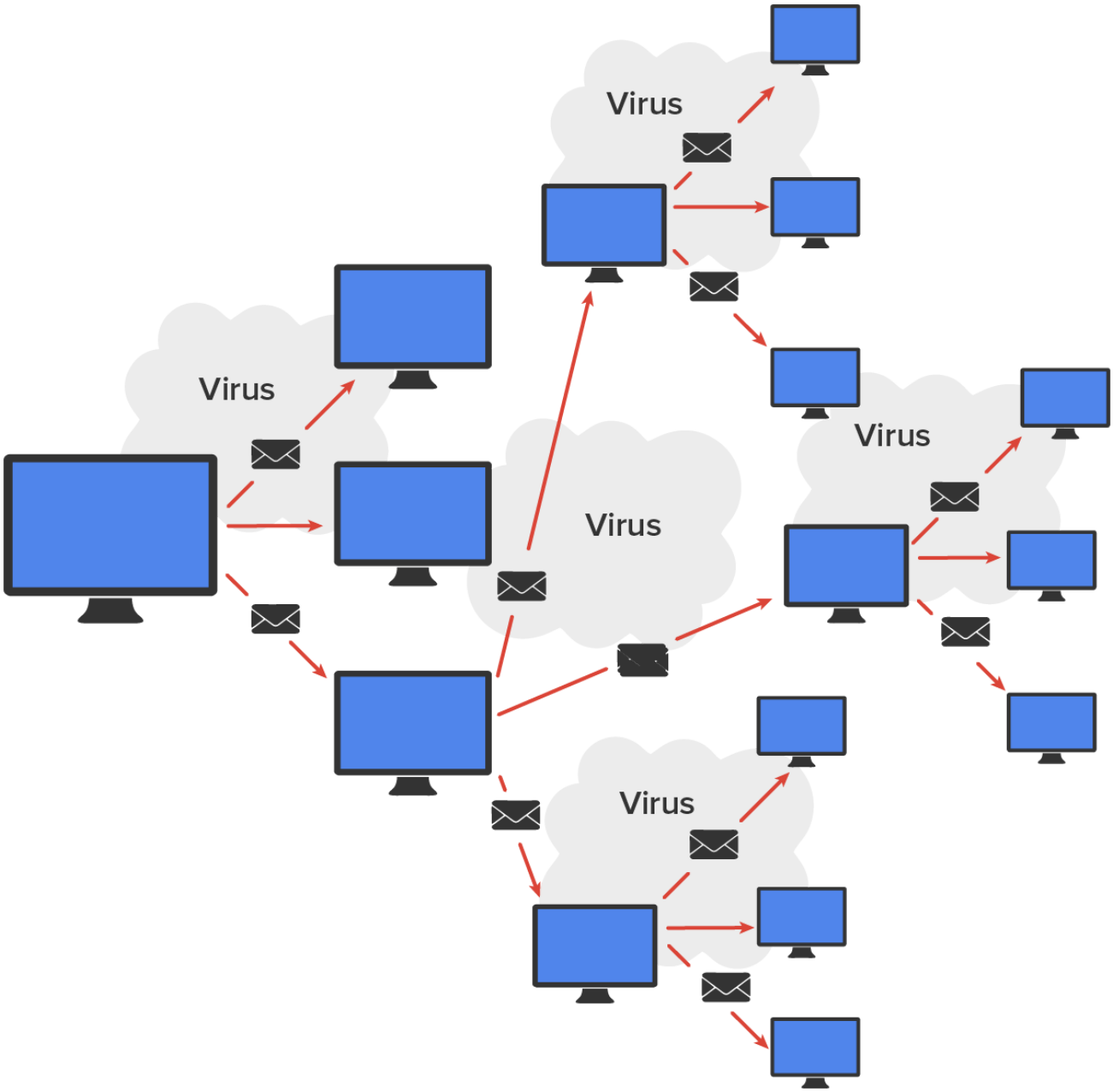
Software developed to harm a computer system.

1a. Viruses

Viruses are probably the best-known threats to your computer’s security because they are the oldest and the most original form of malware. They predate the internet; they used to spread by infecting the boot sectors on removable drives, as well as files downloaded from early online services. In their simplest form, viruses are basically little programs that cause a variety of bad things to happen on your computer, ranging from merely annoying to totally devastating. They can display a message, delete files, or even send huge amounts of meaningless data over a network to block legitimate messages.

KEY CONCEPT

A virus is a code string that embeds itself into an executable file. When that executable file runs, the virus loads itself into memory, and from there it infects other executable files when they run. A key trait of viruses is that they cannot replicate themselves to other computers or systems without running an infected executable, such as one received as an email attachment. The diagram below shows how a virus can spread through an email system.



HINT

There are several different kinds of viruses including file viruses, macro (data file) viruses, and boot-sector viruses. Each type differs slightly in the way it works and how it infects your system.

EXAMPLE A **worm** is a type of malware that can spread without the assistance of the user. A worm is a small program that, like a virus, is used to deliver a payload. One way to help mitigate the effects of worms is to place limits on sharing, writing, and executing programs. However, the real solution is to deploy antivirus and anti-malware software to all devices in the network. This software is designed to identify viruses, **Trojans**, and worms and delete them, or at least quarantine them until they can be removed.

TERMS TO KNOW

Virus

A type of malware which can covertly transmit itself between computers via networks (especially the internet) or removable storage such as disks, often causing damage to systems and data.

Worm

A self-replicating program.

Trojan

Malware that appears to perform or actually performs a desired task for a user while performing a harmful task without the user's knowledge or consent.

1b. File Viruses

A **file virus** attacks executable application and system program files like those with filenames ending in .com, .exe, and .dll. These viruses do their damage by replacing some or all of the target program's code with their own. Only when the compromised file is executed can the virus do its dirty work. It loads itself into memory and waits to infect other executables, propagating its destructive effects throughout a system or network.

TERM TO KNOW

File Virus

A virus that attacks executable application and system program files.

1c. Macro Viruses

A **macro** is a script of commonly enacted commands used to automatically carry out tasks without requiring a user to initiate them. It's roughly equivalent to a very simple executable file; the difference is that it needs another application to execute the commands. Some popular programs, like Microsoft Word and Excel, enable you to create your own personal scripts to perform tasks you do repeatedly in a single step instead of having to enter the individual commands one by one. The application serves as the "engine" that processes the macro's instructions.

A **macro virus** is a computer virus written in a macro language. When the application executes a macro containing a virus, the virus is loaded into memory, and from there it can infect other data files and templates that support macros.

HINT

Macro viruses used to be a big problem in Word and Excel files, but Microsoft has implemented security measures in its applications that reduce the possibility of damage from macro viruses, such as allowing macros only in certain non-default file formats and blocking viruses in files stored in (or originating from) locations that are not trusted.

TERMS TO KNOW

Macro

A string of commands stored in an application's data file, which can be executed from within that application.

Macro Virus

A computer virus written in a macro language.

1d. Boot-Sector Viruses

Boot-sector viruses work their way into the master boot record that is essentially the ground-zero sector on your hard disk where applications are not supposed to live. When a computer boots up, it checks this area to find a pointer for its operating system. Boot-sector viruses overwrite your boot sector, making it appear as if there's no pointer to your operating system. You know you have got this type of virus when you power up the computer and get an error message that says, "Missing Operating System" or "Hard Disk Not Found".

TERM TO KNOW

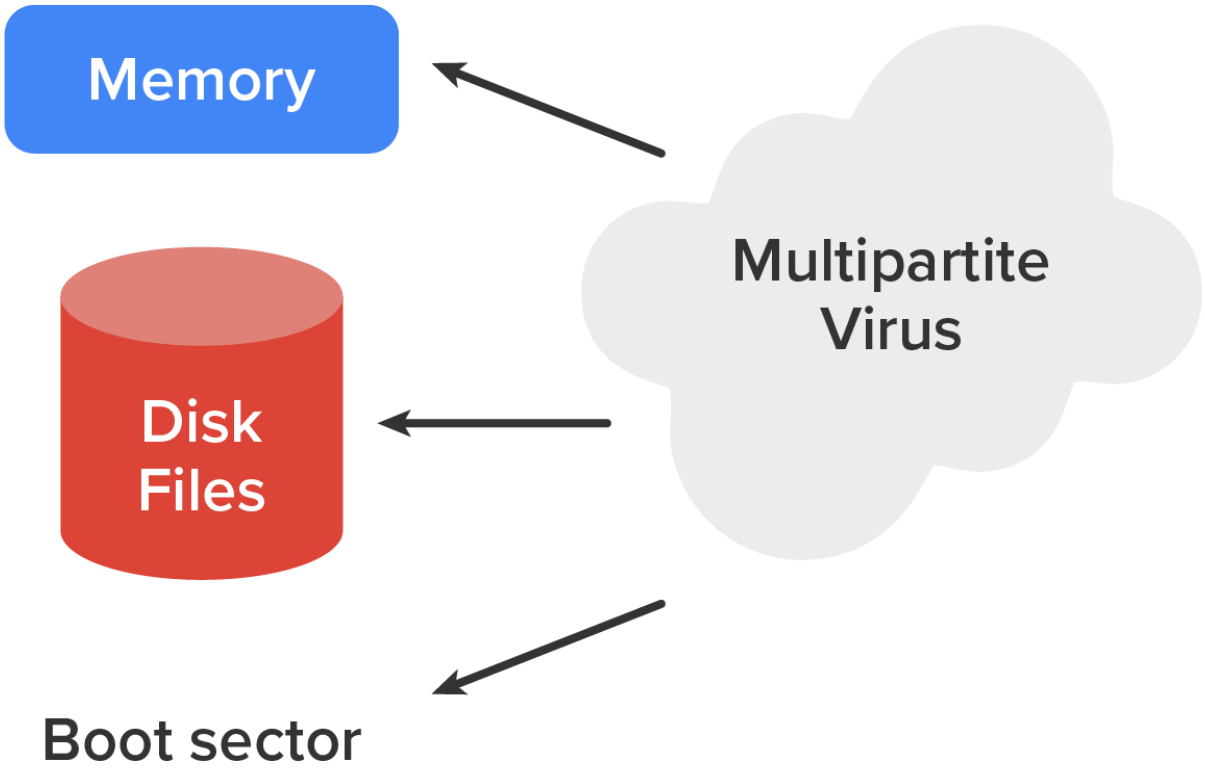
Boot-Sector Virus

A virus that specifically targets the boot sector and/or the Master Boot Record of the host's storage media.

1e. Multipartite Viruses

A **multipartite virus** is one that affects both the boot sector and files on your computer, making such a virus particularly dangerous and exasperatingly difficult to remove.

EXAMPLE The diagram below gives you an idea of how a multipartite virus works. You can see that it is attacking the boot sector, memory, and the disk at once.



While viruses certainly present an ongoing danger to your network, they are not the security professional's only concern. In the following sections, we will cover some other concepts and issues in network security.

TERM TO KNOW

Multipartite Virus

A virus that affects both the boot sector and files on your computer.

1f. Ransomware

Ransomware is a class of malware that prevents or limits users from accessing their information or systems. In many cases, the data is encrypted, and the decryption key is only made available to the user when the ransom has been paid.

TERM TO KNOW

Ransomware

Malware that holds the data of a computer user for ransom, usually requiring or claiming to require payment to restore access.

1g. Logic Bomb

A **logic bomb** is a type of malware that executes when a particular event takes place. For example, that event could be a time of day, a specific date, or it could be the first time you open notepad.exe. Some logic bombs execute when forensics are being undertaken, and in that case, the bomb might delete all digital evidence.

TERM TO KNOW

Logic Bomb

A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

2. Exploits vs. Vulnerabilities

A **vulnerability** is the absence of a countermeasure or a weakness in a countermeasure that is in place. Vulnerabilities can occur in software, hardware, or personnel. An example of a vulnerability is unrestricted access to a folder on a computer.

HINT

Most organizations implement a vulnerability assessment to identify vulnerabilities.

An **exploit** occurs when an attacker takes advantage of a vulnerability and uses it to advance an attack. The following are examples of exploits and vulnerabilities.

TERMS TO KNOW

Vulnerability

A weakness which allows an attacker to reduce a system's security.

Exploit

A program or technique that exploits a vulnerability in other software.

2a. Zero-Day Exploits

Antivirus software uses definition files that identify known malware. These files must be updated frequently, but the update process can usually be automated so that it requires no help from the user. If a new virus is created that has not yet been identified in the list, you will not be protected until the virus definition is added and the new definition file is downloaded. This condition is known as a **zero-day exploit** because it is the first day the virus has been released, and therefore no known fix exists.

Zero-Day Exploit

The act of exploiting a security vulnerability on the same day it becomes publicly known.

2b. Default Passwords/Settings

All network devices are configured with default administrator accounts and their default passwords. These accounts should be disabled and renamed if possible. At the very least, the passwords for these accounts should be changed from the default because they are well known, available in documentation that comes with the product, and also widely available on the internet.

2c. Unnecessary Running Services

Services that are not required to be running on a system should be disabled. Running services present an additional attack surface to the hacker. Once they identify the running services on a machine, they will research all the vulnerabilities presented by those services and attempt to use them to compromise the target.

2d. Open Ports

In the same way that unnecessary services present attack options, so do open ports. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port numbers are used to identify protocols and services and serve as a connection point to a service on a target machine. Port scanners can be used to identify the ports that are open on all machines in a network.

An open port means the device is listening on that port number and is willing to make a connection using that port. Unused ports should be shut down using a firewall.

2e. Unpatched/Legacy Systems

Systems that use older or legacy operating systems and applications may lack the security required in today's networks. These devices may require special protection, such as placing them in a secure VLAN or installing host-based intrusion prevention systems (IPSs). Even modern operating systems and applications will not be secure if they are not maintained by applying updates and security patches as they are released.

HINT

A formal and, preferably, automated process should be set up to ensure that this maintenance is ongoing.

2f. Unencrypted Channels

If it is not clear to you by now, in any situation where sensitive data is being transmitted, you should pay attention to the type of channel across which the data is traveling. When no other method is available, you can use Internet Protocol Security (IPSec), a Network-Layer Protocol suite, to protect any data that resides above the network layer from end to end.

2g. Malicious Users

Damaging activity on your network can come from both inside and outside the network. In a future section, we'll look at malicious users you will encounter and an operation often performed in the execution of their mayhem.

2h. Trusted Users

While we would like to think that all of our own people can be trusted, that is often not the case. Even your "trusted" users can choose to violate security with sufficient motivation.

DID YOU KNOW

The following are among the motives that can turn a trusted user into a malicious user:

- Perceived slight by the company
- Jealousy of other employees
- Monetary reward

The real danger presented by a trusted employee who turns malicious is that the employee is already inside your network and probably knows quite a bit about it. This is the reason for following the principle of least privilege, which prescribes that users be given access only to resources required to do their job.

2i. Buffer Overflow

When programs execute, they write commands into memory, or to a **buffer**. Well-written programs allow a certain location and/or amount of memory space for these commands to execute.

A **buffer overflow** is an event when the amount of data sought to be added to a buffer exceeds the size of the buffer, generally resulting in a catastrophic error if this case has not been anticipated. If a hacker is able to inject a command that overflows the amount of memory allocated and the command is able to execute with the proper security privileges, the hacker could execute commands that would not normally be allowed. They may be able to take control of the machine and create havoc. The way to prevent buffer overflows is to include input validation into programs.

TERMS TO KNOW

Buffer

A portion of memory set aside to store data, often before it is sent to an external device or as it is received from an external device.

Buffer Overflow

An event when the amount of data sought to be added to a buffer exceeds the size of the buffer; generally resulting in a catastrophic error if this case has not been anticipated.

2j. Wireless Threats

The proliferation of wireless communication has introduced a number of security challenges that are unique to the wireless environment. Some of these threats even take advantage of the security measures that have been created to protect wireless networks and hosts. Wireless threats such as cracking of Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) remind us that network attackers never stop evolving their methods and that constant review and adaptation of security measures are required to maintain security in the network.

2k. Backdoors

Backdoors are simply paths leading into a computer or network and are generally a secret means of access to a program or system. From simple breaches to elaborate Trojan horses, attackers can use their previously placed inroads into a specific host or a network whenever they want to unless you can detect them and eliminate their access.

TERM TO KNOW

Backdoor

A secret means of access to a program or system.

2l. Network Reconnaissance

Finally, before breaking into a network, attackers generally gather all the information they can about it because the more they know about the network, the better they can compromise it. This is called network reconnaissance. Attackers accomplish their objectives through methods like port scans, Domain Name Service (DNS) queries, and ping sweeps.

SUMMARY

In this lesson, you learned about specific types of **computer malware** and threats to and **exploits and vulnerabilities** of data networks and computer systems.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

Backdoor

A secret means of access to a program or system.

Boot-Sector Virus

A virus that specifically targets the boot sector and/or the master boot record of the host's storage media.

Buffer

A portion of memory set aside to store data, often before it is sent to an external device or as it is received from an external device.

Buffer Overflow

An event when the amount of data sought to be added to a buffer exceeds the size of the buffer; generally this results in a catastrophic error if the case has not been anticipated.

Exploit

A program or technique that exploits a vulnerability in other software.

File Virus

A virus that attacks executable application and system program files.

Logic Bomb

A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

Macro

A string of commands stored in an application’s data file, which can be executed from within that application.

Macro Virus

A computer virus written in a macro language.

Malware

Software developed to harm a computer system.

Multipartite Virus

A virus that affects both the boot sector and files on your computer.

Ransomware

Malware that holds the data of a computer user for ransom, usually requiring or claiming to require payment to restore access.

Trojan

Malware that appears to perform or actually performs a desired task for a user while performing a harmful task without the user's knowledge or consent.

Virus

A type of malware which can covertly transmit itself between computers via networks (especially the internet) or removable storage such as disks, often causing damage to systems and data.

Vulnerability

A weakness which allows an attacker to reduce a system's security.

Worm

A self-replicating program.

Zero-Day Exploit

The act of exploiting a security vulnerability on the same day it becomes publicly known.