Viruses, Worms, and Buffer Overflows

By Al Lake
LBCC Fall 2014
CS140M

Objectives

- Explain how buffer overflow attacks work
- Describe types of buffer overflows
- Know how to prevent buffer overflows
- Describe viruses and worms and the difference between them
- Know common virus tools
- Understand how antivirus programs work

Contents part of the Certified Ethical Hacker training

Buffer Overflow

- Occurs when a program puts more data into a buffer than it can hold
  - Buffer: Temporary storage area the program uses to store data
- Types of Buffer Overflow:
  - Smashing the stack:
    - Stack: The reserved area of memory where the program saves the return address when a call instruction is received.
    - Organized in LILO structure: First thing placed in the stack is the last thing removed.
    - The attacker can place too much information on the stack or change the value of the return pointer to carry out the attack.
    - The attacker’s code is placed in the buffer.
    - The code could be used to run commands or execute a series of instructions.
  - Heap-based:
    - The memory space is dynamically allocated.

Common Buffer Overflow Attacks

- Morris worm:
  - Uses a buffer overflow in a UNIX program fingerd
- Code Red worm:
  - Affects IIS 5.0 allowing the attacker admin privileges
- SQL Slammer worm:
  - Affects Windows SQL 2000 server and allows execution of arbitrary code
- Microsoft Windows Print Spooler:
  - Enables full access after sending a buffer overflow of 420 bytes
- Apache 1.3.20
- Microsoft Outlook 5.01
- Remote procedure Call (RPC)

Preventing Buffer Overflows

- If the program is developed in-house, the following could be done:
  - Audit the code.
  - Use safer functions.
  - Improve compiler techniques.
  - Disable stack execution.
- For off-the-shelf programs:
  - Turn off application if not used.
  - Apply latest patches.
  - Use a firewall.
  - Test the application.
  - Use the principle of least privilege.

Viruses and Worms

- A type of malware that can cause a wide range of damages such as displaying error messages, crashing programs, or destroying data.
- Viruses place self-replicating code in other programs.
- Worms are viruses that can spread without human intervention.
- Spyware is similar to Trojans and it is used to steal information from the user and consume bandwidth.
Types and Transmission Methods of Viruses

- Viruses require human activity to spread.
- Three basic ways viruses propagate:
  - Master boot record infection:
    - Attacks the master boot record of floppy disks or the hard drive
  - File infection:
    - Relies on the user to execute a file
  - Macro infection:
    - Exploit scripting services installed on the computer

Types and Transmission Methods of Viruses (cont.)

- Types of viruses:
  - Fast infection viruses
    - Spreads quickly and infects all the files it can
  - Sparse infection:
    - Takes longer to infect other files to avoid detection
  - RAM resident infection:
    - Loads itself in RAM
      - The only way boot sector viruses can spread
  - Multipartite virus:
    - Uses more than one propagating method
  - Polymorphic viruses:
    - Changes its signature every time it replicates and infects a new file

Virus Payloads

- Prependers:
  - Place the virus code in the beginning of the infected file
- Appenders:
  - Place the virus code at the end of the infected file
- Virus components:
  - Search routine:
    - Present in all viruses
    - Responsible for locating new files, disk space, or RAM to infect
  - Infection routine:
    - Present in all viruses
    - Responsible for copying the virus and attaching it to a suitable host
  - Payload routine:
    - Is not required
    - Contains the actual virus code
  - Antidetection routine:
    - Helps the virus avoid detection
  - Trigger routine:
    - Launches the payload at a given date and time

History of Viruses

- Lehigh virus (November 1983):
  - Discovered at Lehigh University
  - Hid itself in command.com and counted how many files were infected
  - Wrote data on the floppy disk when the counter reached a predetermined number
- Fred Cohen coined the term computer virus in 1984.
- Ralf Burger created one of the first replicated programs, Virdem, in 1985.
- The Brian virus (January 1986):
  - The first documented computer attack recorded at the University of Delaware
  - Targeted floppy disk's boot sector
- MacMag (March 1988):
  - Developed by Dr. D. D. Davison in 1988
  - Shows drawing of the world on Mac machines
- Score (spring 1988):
  - Another Mac virus reported by EDS
  - Prevents users from saving data
- Strep (Fall 1988):
  - The first well-known Linux virus found in 1988
  - Automatically affected viruses as they are executed by the system user
- Blize (1997):
  - Considered the second Linux virus
  - Locates binary files with write access and overwrite them with its own code

Well-Known Viruses

- Late 1980s:
  - Fred Cohen coined the term computer virus to describe programs that replicate themselves.
  - Ralf Burger created Virdem: An example of self-replicating code.
  - Pakistan programmers released Brian: A master boot record virus.
  - MacMag and Scores: First Mac viruses.
  - Jerusalem virus: Released May 13, 1988 and destroyed files.
  - Stoned and Cascade viruses.
  - RMT (Robert Tappan Morris): First worm released on the Internet.
- Early 1990s:
  - Norton Antivirus released in 1991
  - Chameleon and Tequila: Polymorphic viruses
  - The Good Times hoax

Well Known Viruses cont.

- Mid to late 1990s:
  - Win32/Boora – the first Windows 95 virus
  - Melissa: First macro virus, spread via email and infected the Normal.dot template in Microsoft Word
- 2000 and beyond:
  - I Love You: Hybrid mass mailing worm
  - Anna Kournikova: 2001 VBS hybrid worm attacked Microsoft Outlook
  - Code Red: Exploited jdb buffer overflow vulnerability
  - Nimba: Worm that targets IIS servers
  - Klez: Worm released in 2002 and exploited a vulnerability that enabled an incorrect MIME header to cause IE to execute an email attachment
  - Slammer: Worm that targets SQL
  - MyDoom: Worm that spreads through email
  - Sasser: Worm that exploited IIS's flaws
Virus Tools

- Viruses can be created from scratch or a virus tool kit could be used.
- Virus toolkits:
  - VBS worm generator
  - Virus creation laboratory
  - Macro virus development kit
  - Instant virus production kit
  - Windows virus creation tool kit
  - Smeg virus construction kit

Preventing Viruses

- Install antivirus software.
- Keep virus definitions up to date.
- Don’t open attachments from unknown sources.
- Patch the system regularly.
- Avoid sending attachments.

Antivirus

- A number of antivirus programs are available:
  - Norton Antivirus
  - AVG
  - Trend Micro PC-cillin
  - Sophos Antivirus
  - NOD32 Antivirus
- Antivirus programs use one of the following techniques to check for viruses:
  - Signature scanning:
    - Checks the beginning and end of executable files for known virus signatures
  - Heuristic scanning:
    - Examines computer files for irregular or unusual instructions
  - Integrity checking:
    - Checks files against a database of hash values
  - Activity blocking:
    - Intercepts a virus when it starts to executes and blocks it

Summary

- Explain how buffer overflow attacks work.
- Know common buffer overflow attacks and how to prevent them.
- Know the difference between viruses and worms.
- Describe virus types and transmission methods.
- Be familiar with well-known viruses.
- Know virus tools.
- Explain how to protect against viruses.
- Describe how antivirus software works.

Assignment

- Write a 2-3 page paper with the following:
  - Explain how buffer overflow attacks work.
  - Explain common buffer overflow attacks and how to prevent them.
  - Explain the difference between viruses and worms.
  - Describe virus types and transmission methods.
  - Explain/illustrate some well-known viruses.
  - List some effective virus tools.
  - Explain how to protect against viruses.
  - Describe how antivirus software works.