STUDENT ACTIVITY 2.6_KEY: MALWARE

MTA Course: 98-367 Security Fundamentals
Topic: Malware
File name: SecurityFund_SA_2.6_Key

Lesson Objective

2.6: Understand malware. *This objective may include but is not limited to:* buffer overflow, worms, Trojans, spyware.

Resources, software, and additional files needed for this lesson

- Internet

Directions to the student

Use the Internet to research and define theses famous buffer overflow attacks.

Content

1. Define theses famous buffer overflow attacks: (Answers from Wikipedia)

   Blaster: The **Blaster Worm** (also known as **Lovsan**, **Lovesan** or **MSBlast**) was a computer worm that spread on computers running the Microsoft® operating systems: Windows® XP and Windows 2000, during August 2003. The worm was first noticed and started spreading on August 11, 2003. The rate that it spread increased until the number of infections peaked on August 13, 2003. Filtering by ISPs and widespread publicity about the worm curbed the spread of Blaster.
   On August 29, 2003, Jeffrey Lee Parson, an 18-year-old from Hopkins, Minnesota, was arrested for creating the B variant of the Blaster worm; he admitted responsibility and was sentenced to an 18-month prison term in January 2005.

   Code Red: The Code Red worm was a computer worm observed on the Internet on July 13, 2001. It attacked computers running Microsoft's IIS Web server.
   The Code Red worm was first discovered and researched by eEye Digital Security employees Marc Maiffret and Ryan Permeh. The worm was named the .ida "Code Red" worm because Code Red Mountain Dew was what they were drinking at the time, and because of the phrase "Hacked by Chinese!" with which the worm defaced websites.

Although the worm had been released on July 13, the largest group of infected computers was seen on July 19, 2001. On this day, the number of infected hosts reached 359,000.

Morris Worm: The **Morris worm** or **Internet worm** of November 2, 1988, was one of the first computer worms distributed via the Internet. It is considered the first worm and was certainly the first to gain significant mainstream media attention. It also resulted in the first conviction in the United States under the 1986 Computer Fraud and Abuse Act. It was written by a student at Cornell University, Robert Tappan Morris, and launched on November 2, 1988 from MIT.

Ping of Death: A **ping of death** (abbreviated "POD") is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 56 bytes in size (or 84 bytes when IP header is considered); historically, many computer systems could not handle a ping packet larger than the maximum IP packet size, which is 65,535 bytes. Sending a ping of this size could crash the target computer. In early implementations of TCP/IP, this bug was easy to exploit. This exploit has affected a wide variety of systems, including Unix, Linux, Mac, Windows, printers, and routers. However, most systems since 1997–1998 have been fixed, so this bug is mostly historical.
Generally, sending a 65,536-byte ping packet is illegal according to networking protocol, but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash. In recent years, a different kind of ping attack has become widespread—ping flooding simply floods the victim with so much ping traffic that normal traffic fails to reach the system (a basic denial-of-service attack).

Sasser: Sasser is a computer worm that affects computers running vulnerable versions of the Microsoft operating systems Windows XP and Windows 2000. Sasser spreads by exploiting the system through a vulnerable network port (as do certain other worms). Thus it is particularly virulent in that it can spread without user intervention, but it is also easily stopped by a properly configured firewall or by downloading system updates from Windows Update. The specific hole Sasser exploits is documented by Microsoft in its MS04-011 bulletin, for which a patch had been released 17 days earlier.

Slammer: SQL Slammer is a computer worm that caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic, starting at 05:30 UTC on January 25, 2003. It spread rapidly, infecting most of its 75,000 victims within 10 minutes. So named by Christopher J. Rouland, the CTO of ISS, Slammer was first brought to the attention of the public by Michael Bacarella. Although titled "SQL slammer worm," the program did not use the SQL language; it exploited a buffer overflow bug in Microsoft's flagship SQL Server® and Desktop Engine database products, for which a patch had been released six months earlier in MS02-039. Other names include W32.SQLExp.Worm, DDOS.SQLP1434.A, the Sapphire Worm, SQL_HEL, W32/SQLSlammer, and Helkern