










Chapter 11 - Key Terms

 Term	 Page	 Description
<u>Process</u>	586	A running instance of a program.
<u>Windows process permission</u>	590	User authentication data that is stored in a token and used to describe the security context of all processes associated with the user.
<u>Thread</u>	588	A basic unit that an operating allocates time to.
<u>Job Object</u>	583	Processes grouped together to be managed as a unit.
<u>Thread pool</u>	588	A group of worker threads that efficiently executes asynchronous callbacks for the application.
<u>Fiber</u>		A unit of execution that is manually scheduled by the application.
<u>Static Memory Allocation</u>	588	A process which a program allocates memory at compile time.
<u>Dynamic Memory Allocation</u>	581	A process which a program allocates memory at runtime.
<u>Stack</u>	588	Memory set aside as spare space for a thread of execution.
<u>Heap</u>	582	Memory set aside for dynamic allocation, meaning where you put data on the fly.
<u>VirtualAlloc</u>	589	A specialized allocation of OS virtual memory that allocates straight into virtual memory via reserved blocks.
<u>Virtual Address Space</u>	589	The virtual memory used by processes.
<u>HeapAlloc</u>	582	A function that allocates any size of memory that is requested, meaning it allocates by default.
<u>Malloc</u>	584	A standard C & C++ library function that allocates memory to a process using the C runtime heap.

 Term	 Page	 Description
<u>Windows registration hives</u>	590	A hierarchical database used to store information necessary to configure the system for one or more users, applications, & hardware devices requested, meaning it allocates by default.
<u>Hives</u>	582	Hierarchical folders within the Windows Registry
<u>Windows Management Instrumentation (WMI)</u>	590	A scalable system management infrastructure that was built around a single consistent, standards-based, extensible, object-oriented interface.
<u>Handle</u>	582	An abstract reference value to a resource.
<u>Microsoft Windows services</u>	584	A long-running executable application that operates in its own Windows session.
<u>Log Parser</u>	584	A versatile tool that provides universal query access to text-based data.
<u>Viruses</u>	589	Malicious software that infects a host file or system area to perform undesirable actions such as erasing data, stealing information, and corrupting the integrity of the system. In numerous cases, the virus multiplies again to form new generations of itself.
<u>Worms</u>	590	A virus that replicates itself over the network, infecting numerous vulnerable systems. On most occasions, a worm will execute malicious instructions on a remote system without user interaction.
<u>Mailers & Mass-Mailer Worms</u>	584	A type of worm that sends itself in an email message. Examples of mass-mailer worms are Loveletter.A@mm and W32/SKA.A@m (a.k.a. the Happy99 worm), which sends a copy of itself every time the user sends a new message.
<u>Logic Bombs</u>	584	A type of malicious code that is injected into a legitimate application. An attacker can program a logic bomb to delete itself from the disk after it performs the malicious tasks on the system. Examples of these malicious tasks include deleting or corrupting files or databases and executing a specific instruction after certain system conditions are met.

 Term	 Page	 Description
<u>Exploits</u>	581	A malicious program designed to “exploit” or take advantage of a single vulnerability or set of vulnerabilities. An exploit can be software or a sequence of commands that takes advantage of a vulnerability to cause harm to a system or network.
<u>Downloaders</u>	581	A piece of malware that downloads and installs other malicious content from the Internet to perform additional exploitation on an affected system.
<u>Spammers</u>	587	An attacker who uses a type of malware and whose sole purpose is to send unsolicited messages with the primary goal of fooling users into clicking malicious links or replying to emails or such messages with sensitive information. The attacker seeks to perform different types of scams with the main objective being to make money.
<u>Key Loggers</u>	583	A piece of malware that captures the user’s keystrokes on a compromised computer or mobile device. It collects sensitive information such as passwords, PINs, personal identifiable information (PII), credit card numbers, and more.
<u>Rootkits</u>	587	A set of tools used by an attacker to elevate his or her privilege to obtain root-level access to completely take control of the affected system.
<u>Ransomware</u>	586	A type of malware that compromises a system and then often demands a ransom from the victim to pay the attacker for the malicious activity to cease or for the malware to be removed from the affected system.
<u>Untitled</u>		